SENSIENT®



Sensient Technologies Corporation

Code of Conduct

October 29, 2026

Our Mission

We are an essential business that develops, produces, and supplies critical food, pharmaceutical, and personal care ingredients to the world.

Our Corporate Creed

Always Tell the Truth

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

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

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

Always be Professional

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

Find a Way to Say Yes to Customers

We always find a way to help our customers succeed.

These principles are non-negotiable. They are the foundation of everything we do. In everything we do, we aspire to will the good of each other and our world.

Introduction

The Sensient Code of Conduct (the "Code") sets forth the rules we follow to ensure that we conduct business lawfully, ethically, and safely. Everyone who works for or on behalf of Sensient must maintain high standards of professional and personal ethics while performing his or her work.

The Code of Conduct applies to:

- full-time or part-time employees and officers;
- interns, apprentices, and temporary and agency employees while working for or on behalf of Sensient; and
- members of the Board of Directors and Scientific Advisory Committee. [1]

For convenience, we refer to all these people as "Employees." Each Employee is responsible for understanding and following the Code.

The Code does not address all of the laws we encounter as we do business. Nor is the Code an employment contract. The Company may modify or eliminate parts of the Code or adopt a new Code at any time and will use reasonable efforts to communicate such changes to Employees. If you have questions about the Code, please contact the Legal Department.

The Company works diligently to prevent and detect unethical or unlawful conduct by its Employees. Any Employee who is found to have violated the Code is subject to discipline, up to and including immediate termination. Supervisors and managers of the disciplined Employee may also be subject to disciplinary action or termination if they have failed to properly oversee Employee conduct or if they have retaliated against Employees who report violations. The Code is enforced on a uniform basis for all Employees, without regard to their position within the Company.

The Company conducts periodic training on the Code 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.

Reporting Possible Violations ("Whistleblower Procedures")

Employees must immediately report possible violations of law or the Code using one of the reporting channels listed below or to their supervisor or a Human Resources representative.

Any supervisor or Human Resources representative who receives a report of a possible violation of law or the Code must immediately report the possible violation to the General Counsel.

[1] This Code also applies to all contractors while they are engaged in work for Sensient.

Sensient Technologies: Level 4 External

Former and prospective Employees are also invited to make reports. Employees must cooperate fully in any investigation of a potential violation.

A failure to report a potential violation of law or the Code within one business day is a violation of the Code. The Company's goal is to remediate any potential violation as quickly as possible.

All reports must be reviewed promptly by the General Counsel, and for financial matters, by the Director, Internal Audit.

You can make a report by:

- Telling your supervisor or local Human Resources representative;
- Calling, emailing, or writing to the General Counsel or Director, Internal Audit in the Milwaukee Office;
- Calling the hotline at +1 414-921-4487 and leaving a message; or
- Using the concerns form at https://sensient.sharepoint.com/sites/Legal/SitePages/My-Legal-Concerns.aspx.

A report:

- Can be made confidentially or anonymously;
- Can be verbal or written;
- Must be complete and made to the best of your personal knowledge;
- Should include sufficient information about the complaint or concern so that it can be properly investigated; and
- May (but is not required to) include your name, contact information, and your relationship with the Company. [2]

Where confidentiality has been requested, the Company will keep your report confidential to the fullest extent required by law.

All reports of possible violations will be promptly investigated and resolved as appropriate under the direction of the General Counsel with the support of Internal Audit and Human Resources as appropriate. All investigations will be conducted in compliance with applicable laws.

[2] The Company will only use this information to the extent necessary to investigate a report and will otherwise protect such information, consistent with all applicable privacy laws. This will help the Company to focus its investigation of the matter and, when appropriate, report back concerning its resolution of the complaint or concern.

The General Counsel will report the results of all investigations to the Audit Committee of the Board of Directors on a quarterly basis. The Chief Executive Officer will provide anonymized reports to Employees regarding violations of the Code on a regular basis. The General Counsel will also conduct periodic reviews of reporting and violation trends and implement measures as needed to prevent the recurrence of such violations.

No Retaliation for Reporting

The Company will not retaliate against anyone who makes or assists someone else in making a good faith report about a possible violation of regulation, law, or the Code. Retaliatory acts are all actions attempted, threatened, or undertaken that aim to jeopardize a reporting Employee's interests or rights in a legally impermissible manner. Retaliatory acts include dismissing, demoting, suspending, disciplining, threatening, harassing, intimidating, sanctioning, or discriminating against the reporting Employee. It is a crime in the United States, the European Union, and elsewhere to retaliate against a person for providing truthful information to the Company's internal compliance and reporting system or to a government official or agency.

Anyone who retaliates against an Employee for reporting a possible violation of the Code will be terminated. The prohibition of retaliation assumes that individuals will act in good faith in bringing forward a concern. Anyone who makes a maliciously false report or otherwise acts in bad faith in reporting a concern will be subject to disciplinary action, up to and including termination.

Reporting Possible Accounting Violations

Reports of actual or suspected violations relating to accounting, auditing, internal controls, or compliance matters ("Compliance Matters") will be reported to the Chairman of the Audit Committee and will be reviewed and investigated under Audit Committee direction and oversight. Investigations will be conducted by such persons as the Audit Committee determines to be appropriate, which may include the General Counsel, Director, Internal Audit, and outside legal, accounting, or other advisors.

The Company will take prompt and appropriate corrective action as warranted in the judgment of the Audit Committee.

The Audit Committee will retain as part of its records all reports of complaints or concerns regarding Compliance Matters and their treatment. These records will be anonymized in compliance with data privacy laws.

The General Counsel will assist the Audit Committee by maintaining files regarding all reports and tracking their receipt, investigation, and resolution, and will prepare a periodic summary report thereof for the Audit Committee.

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

Special Reporting Rules in the United States

In the United States, Employees who believe that they have been retaliated against for providing information to a federal agency or Congress, or for providing information about suspected fraud to a supervisor, 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.

Nothing in this Code is intended to prohibit you (with or without prior notice to the Company) from (1) exercising any protected right to file a charge or complaint with the U.S. Congress or any governmental agency charged with enforcement of any law, or (2) exercising any protected right to participate in an investigation or proceeding conducted by such agency or recovering any award offered by such agency associated with such charge or complaint, or (3) making any other disclosures protected by applicable whistleblower statutes. Nothing in this Code precludes 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 limits the rights of those Employees to participate in any investigation by the National Labor Relations Board.

Employees should keep in mind that it is a crime in the United States to willfully make a materially false statement to a government agency.

Furthermore, Employees are advised that they cannot be held criminally or civilly liable under any federal or state trade secret law for the disclosure of a trade secret that is (1) made in confidence to a federal, state, or local government official, either directly or indirectly, or to an attorney; and solely for the purpose of reporting or investigating a suspected violation of law; or (2) in a complaint or other document filed in a lawsuit or other proceeding, if such filing is made under seal. An Employee who files a lawsuit for retaliation by the Company for reporting a suspected violation of law may also disclose the trade secret to his or her attorney and use the trade secret information in the court

proceeding, provided that the Employee (1) files any document containing a trade secret under seal; and (2) does not disclose a trade secret, except pursuant to a court order.

Special Reporting Rules under National Laws Implementing EU Directive 2019/1937

Whistleblowers who make truthful reports cannot be subject to civil claims by the Company and cannot be penalized for accessing the information they disclose unless gaining such access was an illegal act. The Company will keep the whistleblower's report and identity confidential except that the Company will report to its Audit Committee regarding the substance of all whistleblower reports, the channel in which the report was made, and any remedial action taken by the Company. The requirement that Employees make reports of any possible violations of law or the Code to the Company does not preclude an Employee from making a report to the competent government authorities or, as a last resort or in cases of imminent danger to the public interest, to the media.

Accounting Matters

Senior Financial Officers [3] must follow specific standards and procedures to ensure that Company business is conducted in a lawful and ethical manner. Employees are responsible for following the Company's Internal Controls (see below).

Disclosure Controls and Procedures

U.S. federal and state securities laws impose continuing disclosure requirements on the Company. We must file regular reports (the "Reports") with the SEC and the New York Stock Exchange (NYSE) and disseminate these Reports to our shareholders.

These 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 that 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 understand and strictly follow such controls and procedures in the preparation of Reports.

[3] Senior Financial Officers include the Chief Executive Officer, Group Presidents, Chief Financial Officer, principal accounting officer, controller, finance directors, and all other persons performing similar functions anywhere in the world for the Company.

All Senior Financial Officers and all representatives who assist the Company in making Reports, communications, and other disclosures [4] will ensure that such Reports, communications, and other disclosures (i) are full, fair, timely, factual, accurate, and understandable, and (ii) meet all legal requirements.

This policy applies to all public disclosures 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 (i.e., money and property) 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 here.

It is the responsibility of the business unit, Group, and Corporate management, including Senior Financial Officers, to establish a proper control environment and procedures. Local management must take measures and actions necessary to ensure that Employees understand and comply with the procedures for appropriate internal controls. In addition, it is the responsibility of the business unit, Group, and Corporate Controllers/Finance Directors, to approve, on a monthly basis, the control procedures and activities summarized in the Monthly Financial Statement Certification.

An effective system of internal controls includes 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 is required at all times.

The Internal Audit Department will monitor compliance with established internal controls at each location; review the adequacy, appropriateness, and efficiency of the control procedures; and make recommendations to management for improvements in these procedures. Any questions regarding the system of internal controls should be addressed to the Director, Internal Audit.

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

[4] Reports, communications, and other disclosures means written disclosures, oral statements, visual presentations, press conferences, and media calls.

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 must 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 Employees understand and comply with these accounting and auditing laws, standards, controls, and practices.

Antitrust Laws

Employees must comply with the Company's **Antitrust Compliance Policy (Appendix).**

Antiboycott Laws

Under U.S. law, [5] the Company and its Employees are prohibited from:

- Refusing to do business with the subject of the boycott, including using, or agreeing to use, blacklists;
- Discriminating 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.

Authority to Act on Behalf of the Company

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

[5] The U.S. Export Administration Act and the 1976 Tax Reform Act ("Antiboycott Laws"). 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 Legal Department immediately.

All nondisclosure/confidentiality agreements and contracts (whether with a customer or vendor) must be submitted to the Legal Department for review and approval.

Only Executive Officers have the authority to initiate non-routine contact with, or negotiate with, a government regulator (e.g., the FDA) on behalf of the Company. Routine regulatory interactions (such as responding to inspections, filing required routine reports, and similar operational matters) may be handled by appropriately authorized Employees in accordance with applicable Company procedures.

Bribery

Sensient does not pay bribes of any kind and will not do business with anyone who does. Employees are required to comply with the **Anti-Bribery Policy (Appendix).**

Communicating Product Safety Matters to the CEO

Employees must ensure that any product safety issue is communicated to the CEO. Employees can fulfill this obligation by communicating such matters to the Vice President, Product Quality & Safety or their General Manager.

Communications with Analysts and the Media

Only the Company's Chief Executive Officer, Chief Financial Officer, and Treasurer are authorized to speak with securities analysts, investors, and investment professionals.

The Company's CEO, CFO, Treasurer, and individuals designated in writing by the CEO are the only authorized contacts for official statements or responses to the media concerning our Company.

Nothing in this Code precludes 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 limits the rights of those Employees to participate in any investigation by the National Labor Relations Board.

Company Property

Employees must protect the Company's property and assets and ensure their efficient use. Any Employee who intentionally steals or misappropriates, or intentionally or negligently damages or wastes, Company property will be subject to discipline up to and including termination. Falsely reporting working hours constitutes time theft. Any suspected incident of fraud or theft must be reported immediately as described in the Reporting Possible Violations section above.

Confidentiality

Employees must protect Sensient's Company Confidential Information and comply with the **Company Confidential Information Policy (Appendix)**. Members of the Board of Directors must comply with the **Director and SAC Confidentiality Policy (Appendix).**

Conflicts of Interest

Conflicts between an Employee's personal or private interests and those of the Company are prohibited unless a written waiver is granted by the General Counsel.

A potential conflict of interest exists when an Employee has any position with, or a substantial interest in, another business that might reasonably appear to conflict with the proper performance of the Employee's job responsibilities or independent and objective judgment with respect to transactions between the Company and the other business. For example, if an Employee engaging a vendor has any familial relationship (including relationships formed through marriage) or close friendship with the vendor there is a conflict of interest. Accordingly, such conflicted Employee must disclose that relationship to his or her supervisor and may not control the selection of such vendor. If such vendor is nonetheless selected after an appropriate review by non-conflicted Employees, the conflicted Employee may not be the final approver for any invoice from such vendor.

Employees must comply with the Company's **Conflict of Interest Policy (Appendix).**

An Employee's off-duty work must not interfere with the Employee's ability to perform his or her job effectively and must not adversely affect productivity in the workplace.

Cybersecurity

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

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

- On an annual basis, the Board of Directors must define high-risk cybersecurity areas for the Company and implement comprehensive programs to address these risks. High risk areas will be reviewed and revised as needed.
- Management must report at least twice annually to the Board of Directors on cybersecurity progress and effectiveness.

- The Company will maintain an executive-level steering committee (including the CEO, CFO, Group Presidents, General Counsel, and CIO) to meet monthly and provide oversight of the Cybersecurity Program.
- The Company will conduct mandatory annual employee training programs, quarterly cyber executive incident response simulations, and regular cyber penetration testing.
- The Company will make investments as required in its technical capabilities in all areas of security.

Electronic Communications

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

Employees must comply with these rules when accessing or using the ECS [6]

- **Ownership.** The Company owns its ECS and everything on it.

- **No privacy.** Employees have no rights of privacy when using the ECS. The Company may choose to share the contents of its ECS with law enforcement.

- **Access, monitoring, and searches.** The Company reserves the right to monitor, access, and search the ECS. The Company reserves the right to inspect and search all computers, electronic devices, and components of the ECS found on Company property without notice to ensure that Employees are complying with Company policies. These Company rights will be exercised in accordance with applicable law.

- **No inappropriate use.** Employees may not use the ECS in a harassing, illegal, or defamatory manner. Employees may not use the ECS to send or receive improper messages such as sexually explicit or pornographic messages or images (including actual or attempted meetings or assignations with sex workers, unwelcome propositions, requests for dates, or love letters); profanity, obscenity, slander, or libel; ethnic, religious, sexual, racial, or other slurs; messages containing partisan political commentary unrelated to Company business or working conditions; or any other message that could be construed as harassment of others.

[6] These rules do 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. For purposes of this rule, such protected activities are specifically excluded from the definition of the word "political" as used herein.

- **Pornography, sexually explicit, and other sexually inappropriate material.** Employees may not view, download, or possess any pornographic, sexually explicit, or other sexually offensive material on the ECS.

- **Solicitation.** Employees may not use the ECS for illegal activities, personal commercial activities, or to promote religious or political causes.

- **Confidential information.** Employees may not improperly disclose confidential Company information in any manner, including via the ECS.

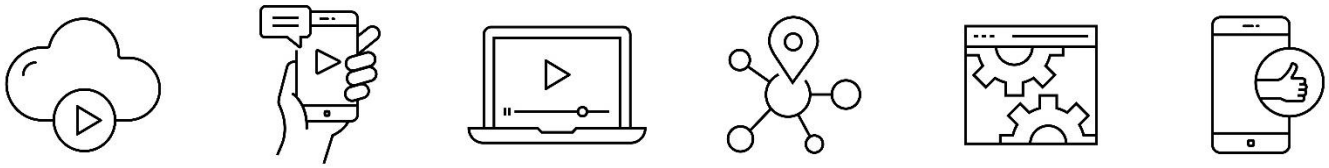
- **Copyrights, trademarks, and patents.** Employees must not violate copyrights, trademarks, or patents via the ECS or otherwise.

- **No unapproved software.** Only Company-authorized software may be used on the ECS. Employees may not take any action to prevent the Company from accessing or recovering any encrypted information.

- **Text messages.** Company-related text messages should only be sent through Company-issued cell phones or other ECS systems such as Teams.

- **Personal devices.** Employees are not allowed to use personal electronic devices to access the Company's ECS unless the device is approved by the Company and used for Company-authorized purposes.

- **Personal use.** Incidental and occasional personal use of the ECS is allowed, but such use is subject to the Code, and any resulting messages and data are the property of the Company. This personal use is allowed when it does not interfere with any Employee's work performance, unduly impact the operation of the ECS, or violate the law, the Code, or any Company policy.



Company Confidential Information (CCI)

CCI is secret information about Sensient's business, such as:

Scientific, technical, and engineering information	Financial, sales, and operational data	Strategies and business plans	Customer and supplier lists and order histories

Even if you wrote or created the CCI, it belongs to Sensient, NOT YOU.



DO NOT put CCI on a flash drive, thumb drive, GoogleDocs, or any other external platform or device.



DO NOT send CCI to a personal email address.



DO NOT attach CCI to a draft email in a personal email account.



DO NOT enter CCI into ChatGPT or any open AI system.



DO NOT take a picture of CCI (documents, PowerPoints, equipment, etc.).



DO NOT take CCI with you after your employment at Sensient ends.



Our IT Security Team has powerful tools to detect misuse of CCI. If you violate the CCI rules, you will be caught, you will be fired, and the Company will contact law enforcement, if appropriate.

Environment, 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. Each Employee and each facility will comply with all applicable environmental, health, and safety ("EHS") laws and regulations. All Company facilities will be operated in a manner to protect the health of our workers through the adoption of appropriate work practices and to avoid harm to the environment and promote sustainability through the adoption of appropriate environmental management systems. Violations of Company EHS policies or EHS laws and regulations are violations of the Code.

Employees will be appropriately trained and are required to perform their jobs in a safe manner. Employees may not:

- Report for work or work while drunk, high, or otherwise impaired;
- Use, possess, distribute, or receive intoxicating beverages or controlled substances (other than properly prescribed medicines used consistent with medical instructions) while working; or
- Use intoxicating beverages or controlled substances off premises where such activity adversely affects work performance, safety, or the reputation of the Company.

All employment offers are contingent upon passing a pre-employment drug test, to the extent permitted by applicable law.

Corporate EHS Department

The Corporate EHS Department establishes EHS policies, standards, and initiatives; oversees, monitors, and measures EHS performance; promotes awareness of EHS issues; consults with internal and external stakeholders and outside consultants as required; and conducts EHS compliance audits. Under the guidance of the Legal Department, the EHS Department provides definitive interpretation of EHS laws and regulations.

Group Presidents, General Managers, and Facility Managers

Group Presidents and General Managers are responsible for ensuring compliance with applicable EHS laws and regulations and for implementing Corporate EHS policies and programs at their facilities. Facility Managers are responsible for developing and implementing procedures to ensure that all Company activities and facilities remain in compliance with Corporate policies and applicable EHS laws and regulations. Facility Managers are also responsible for emergency preparedness, hazard identification, and risk assessment. While remaining personally responsible for compliance, Facility Managers may delegate specific responsibilities to other facility personnel.

EHS Audits

The Corporate EHS Department will schedule periodic third-party EHS compliance audits. General Managers will promptly implement corrective actions as required.

Consequences of Non-Compliance

The consequences of non-compliance with EHS laws and regulations can be severe, including harm to our employees and/or surrounding communities; pollution of the environment; significant civil and criminal penalties for the Company; prison time, fines, and/or penalties for Employees; closure of our facilities; and adverse publicity.



Sensient Technologies: Level 4 External

Code of Conduct

Integrity	Safety	Professionalism	Say Yes to Customers
Do not lie, cheat, or steal	We make safe products in safe and secure facilities	We treat everyone with respect	Find a way to help our customers succeed

The Code of Conduct applies to everyone who works at Sensient, at all times. If you break one of the Three Rules, you will be fired.

DO NOT violate lockout-tagout (LOTO) procedures.





DO NOT work under the influence of drugs or alcohol.

DO NOT sleep on the job.





DO NOT lie. Tell the truth in what you say and on the forms you sign (examples: HACCP & CIP forms).

DO NOT work without personal protective equipment (PPE).





DO NOT engage in threatening or aggressive behavior. NO fighting.

DO NOT harass anyone. NO insults or name calling. NO sexual comments or jokes. NO unwanted touching



Equal Employment Opportunity

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

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

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

The Company will administer all policies, benefits, and programs, including but not limited to those relating to interviewing and selection, compensation, promotion, transfer, layoff, recall, and training, on a nondiscriminatory basis and in accordance with applicable law and the Corporate Creed. The Vice President, Human Resources and his or her staff are responsible for developing and administering procedures designed to ensure compliance with this section of the Code.

Export Controls

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

It is the Company's policy to comply with all applicable U.S. and non-U.S. export control statutes and regulations as summarized in the **Sensient Technologies Corporation Export Compliance Policy**. Employees must fully comply with the **Export Compliance Policy,** and violations will be punishable as provided in the Code. It is critical to consult with the Legal Department before even discussing a possible sale or purchase of any product that may be subject to U.S. and/or non-U.S. export controls.

Facility Visits

Facility visits are governed by the **Sensient Physical Security Policy.**

Fair Dealing

The U.S. Federal Trade Commission Act prohibits "unfair methods of competition" and "unfair or deceptive acts or practices," which includes any business conduct that deceives or misleads the consuming public. No Employee may engage in unfair methods of competition or unfair or deceptive acts or practices. Every Employee must endeavor to deal fairly with the Company's customers, suppliers, competitors, and other Employees. No Employee should take unfair advantage of any person through manipulation, concealment, abuse of privileged information, misrepresentation of material facts, or any other unfair-dealing practice. Misuse of someone else's intellectual property constitutes unfair dealing.

Fraternization

Supervisors and managers may not carry on a romantic relationship [7] with any subordinate. In addition, Company officers, the highest-ranking manager at each of the Company's locations, and Human Resources staff are prohibited from carrying on a romantic relationship with any Employee. The Company has no desire to interfere with the private lives of its Employees, but where off-duty conduct may affect the work environment, the Company will take appropriate action to protect its interests.

Any Employee engaged in a romantic relationship with another Employee is required to notify the Employee's Human Resources Manager or Director, or the Vice President, Human Resources. This section of the Code is not intended to discourage friendship and camaraderie between personnel, but rather, to ensure that personal relationships do not interfere with workplace responsibilities, create conflicts of interest, or result in favoritism (real or perceived).

Governmental Inspections, Inquiries, and Investigations

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

Employees must comply with the **Governmental Inspections Manual**, which contains procedures to be followed during the course of governmental inspections, including procedures for internal notification and reporting.

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.

[7] The term "romantic relationship," includes, but is not limited to, casual and serious dating, sexual involvement, cohabitation, and any other behavior normally associated with romantic or sexual relationships.

Any Employee who receives notice of a governmental inquiry or investigation (e.g., request for information concerning compliance status of the Company or a Company facility, notice of noncompliance, notice of violation, etc.) must immediately communicate such information to his or her responsible Plant, Facility, or General Manager. The responsible manager must immediately notify the Legal Department of the inquiry or investigation. The Legal Department will oversee any inquiry or investigation in which the Company becomes or might become involved.

Any Employee who receives a criminal or civil subpoena requesting a response from the Company must immediately refer such requests to the Legal Department. Company lawyers are the only individuals authorized to respond on behalf of the Company.

Employees are reminded that lying in the course of a governmental investigation is a crime.

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 and Violence

The Company does not tolerate violence. Accordingly, any Employee who is found to have assaulted, battered, or threatened any person, regardless of where such action occurs, will be terminated.

- Assault includes using, brandishing, or threatening to use any weapon against any person, regardless of where occurring.
- Battery includes any intentional physical touching that is harmful or offensive, regardless of whether injury results.
- A threat means a statement of present or future intent to assault, batter, or otherwise physically harm someone. ***See* Sensient Physical Security Policy**.

The Company prohibits intimidation and harassment.[8] 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 vendors). Intimidation and harassment include, but are not limited to:

[8] 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.

- Physical or mental abuse;
- Racial, ethnic, or religious insults or slurs;
- Unwelcome sexual advances or touching;
- Sexual comments, jokes, stories, or innuendos, including sexual gestures;
- Requests for sexual favors as a condition of employment or affecting any personnel decision such as hiring, promotion, compensation, or termination;
- Display of sexually explicit or otherwise offensive posters, calendars, or materials; sending sexually explicit or suggestive electronic communications;
- 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.

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 because they can be held legally liable as an individual. These rules apply 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 has 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 non-Employees who engage in such behavior may be limited, we are committed to taking appropriate action to protect our Employees. If an Employee becomes aware of such behavior, he or she must immediately report it. *See* **Reporting Possible Violations.**

- If any Employee believes that he or she has witnessed or has been the subject of prohibited harassment or retaliation:
- If not comfortable speaking to the person who has engaged in the inappropriate behavior, or if the inappropriate behavior does not stop, or if the Employee is not satisfied with the result of the discussion with the offender, the Employee must immediately report the inappropriate conduct as provided under **Reporting Possible Violations**.
- Any report of sexual harassment received by any supervisor or manager must be immediately reported to the General Counsel.

It is important that the Employee immediately inform the Company about the inappropriate conduct, because the Company cannot do anything to remedy the problem if it does not know that it exists.

Insider Trading

Employees may buy or sell stock in the Company, provided:

(1) The Employee is not in possession of material non-public information; and
(2) The purchase or sale occurs during the 30 day "window" period following the Company's public earnings release; and
(3) For executive officers and directors, their transactions are properly reported to the SEC.

Even though this type of trading may be legal, it is essential that any officer or director buying or selling Company stock do so only in strict compliance with the Company's **Insider Trading Policy** (Appendix).

Trading in a stock when in possession of material nonpublic information is illegal. This type of illegal insider trading includes:

- Where any Employee buys or sells stock when in possession of material nonpublic information for his or her own benefit; and

- Where any Employee provides material nonpublic information to another person who trades – even if the person providing the information does not know about the trade - based on that information. This latter scenario is known as "tipping."

These rules can also apply to the stock/securities of our customers, suppliers, and even competitors and peer companies.

What constitutes material nonpublic information is a complex legal question that depends on the specific facts of a particular situation. Generally, information is "nonpublic" if it has not been disseminated to the general public and is "material" if an ordinary investor would most likely take that information into account when deciding whether to buy, sell, or hold securities. Material information includes information about the Company's earnings, a merger or acquisition in which the Company is involved or affected, the launch of a new product, the entry into or loss of a major contract, and an actual or a suspected cybersecurity risk or incident. These examples are not exhaustive, and all Employees may be in possession of material non-public information from time to time.

Employees should never communicate material nonpublic information to anyone outside the Company and should only discuss with other Employees on a "need-to-know" basis.

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 Communications and Director and SAC Confidentiality policies:

- Employees must maintain the confidentiality of material nonpublic information and not disclose it to any third party, except where such disclosure is part of an official Company statement distributed to the general public (e.g., a press release).

- Employees may not 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 outside the "window period," which is described in the Appendix to the Code.

- In general, regular, ongoing stock purchases in the Company's Savings Plan, Employee Stock Ownership Plan, and Employee Stock Purchase Plan are not subject to these prohibitions. However, any change in election or other reallocation of funds involving Company stock under such a benefit plan is subject to the Company's prohibitions against illegal insider trading and cannot be completed while in possession of material nonpublic information (and, for officers, must be completed in a window period).

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

Inventions

Everything Employees create during the course of their employment at Sensient belongs to Sensient, except to the extent otherwise required by applicable state or national law.

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

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

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

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

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

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

Legal and Ethical Compliance

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

its Employees may assist any third-party in violating the laws of any country or location in which we operate.

Global human rights are fundamental to the operations of Sensient's business. Human rights are rights, freedoms, and standards of treatment regarded as belonging to all persons. Sensient respects and supports internationally recognized human rights and is committed to high standards of ethics, honesty, and integrity and demonstrating respect and dignity for one another and those with whom we do business. The Code was developed with consideration for recognized global standards and guidelines, including the principles found in the International Bill of Human Rights, the UN Guiding Principles on Business and Human Rights, and the ILO Declaration on Fundamental Principles and Rights at Work.

We also seek to work with suppliers that employ practices that meet or exceed applicable laws. These requirements and expectations for ourselves and our suppliers include, without limitation, the matters described below. In the event local standards on a matter do not exist or do not meet these ethical standards, the Company and our suppliers must nevertheless establish employment practices and will apply U.S. standards where appropriate while complying with local law. Compliance with the law and observing our ethical obligations are absolutely essential conditions for fulfilling our duties to each other, our customers, and society as a whole.

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

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

- **No child labor.** The Company prohibits the exploitation of children and use of illegal child labor. Work by children under the age of 15 years (or any higher age established by applicable law) is strictly prohibited. Human Resources must ensure that Employees are legally eligible for employment and meet the applicable minimum legal age. Human Resources will maintain, in accordance with applicable laws, verifiable documentation of each employee's date of birth, or some legitimate means of confirming each employee's age. Concerns related to child labor may be reported confidentially and without retaliation through

Human Resources or by contacting the Corporate Legal Department at +1 414-921-4487. If it is identified that the Company has either caused or contributed to adverse impacts on children's rights:

  - The child shall be removed immediately from hazardous or unlawful work;
  - A remediation plan shall be implemented in the best interests of the child, in consultation with the child and parent or guardian; and
  - The remediation plan shall support the child's access to education or vocational training.

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

- **Nondiscrimination.** The Company values the dignity of each person as an individual and provides equal employment opportunities to all people based upon individual merit alone. The Company will not discriminate based upon any characteristic protected now or in the future by applicable law. We will not tolerate discrimination by anyone with whom we do business.

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

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

- **Compliance with U.K. Modern Slavery Act.** The Company and our suppliers will comply with the requirements of the U.K. Modern Slavery Act of 2015 and take steps to ensure that slavery, servitude, forced or compulsory labor, and human trafficking are not present in the Company or its supply chain. Slavery is where ownership is exercised over a person; servitude involves the obligation to provide services imposed by coercion; forced or compulsory labor involves work or service exacted from any person under the menace of a penalty and for which the person has not offered himself or herself voluntarily; and human trafficking concerns arranging or facilitating the travel of a person with a view to exploiting him or her. If the Company finds any supplier has committed any of these prohibited acts, the Company will promptly terminate its commercial relationship with that supplier.

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

- **Environment, health, and safety.** The Company is committed to sound EHS practices. Safety awareness and procedures, environmental compliance, waste minimization, and resource conservation are primary objectives. We expect the same commitments from our suppliers. *See* **EHS Policy.**

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

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

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

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

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

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

- **Free, prior, and informed consent (FPIC).** The Company is committed to following the principles of free, prior, and informed consent (FPIC) of indigenous peoples for property or land negotiations and requires the same commitment of our suppliers. All forms of land grabbing are prohibited. Adherence to the principles of free, prior, and informed consent of indigenous peoples is required in all negotiations for property or land, including the use of and transfers of it.
-

Land rights of individuals, indigenous people, and local communities affected by sourcing practices, supply chains, and operations are respected.

- **Human Right to Water.** The Company acknowledges that every human being has the right to safe, clean, affordable, and accessible water adequate for human consumption, cooking, and sanitary purposes.

Legal Services and Contact by Outside Lawyers

The Legal Department provides legal advice and guidance to the Board and Company management and works to ensure the Company's compliance with applicable laws. The Legal Department has the sole authority to engage and supervise outside legal counsel. The Legal Department will keep the Company's Board and management advised of pertinent developments in the law.

If any Employee is contacted by an outside attorney, he or she should immediately direct such attorney to contact the Legal Department.

Manufacturing

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

- Purchasing programs will be established to procure necessary manufacturing materials at the lowest cost consistent with quality and service standards.
- Equipment and facilities maintenance programs will be established by business units and will conform to established engineering and EHS standards.
- Programs will be established by business units to ensure proper compliance with all federal, state, and local regulations regarding manufacturing and distributing food products in compliance with the **Product Safety** section of the Code.
- 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. *See* **Physical Security Policy.**
-

- The Treasury Department will maintain adequate insurance coverage at all times to protect the Company from undue loss.

Political Activities

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

Product Safety

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

Any Employee with concerns about the safety of Company products must immediately report that concern to his or her General Manager, who will notify the Company's CEO. If the General Manager is unavailable or does not appropriately address the issue, the Employee must report the concern directly to the CEO.

The Company is committed to providing only products that are safe for consumers, properly labeled, and comply with all applicable legal requirements, including food safety and labeling requirements. [9] The Company is absolutely committed to compliance with all of these requirements for food safety and integrity, and Employees are expected and required to perform their work in a manner that reflects unqualified commitment to these principles.

Products manufactured or supplied by the Company that do not meet all applicable safety and legal requirements will not be sold. Any decision to recall product manufactured by the Company must be made in accordance with the **Sensient Technologies Corporation Product Safety and Recall Manual**, and other applicable Company food safety manuals and guidelines.

Records Retention

Employees must comply with the Company **Records Retention Policy (Appendix)**.

[9] For example, U.S. Food & Drug Administration law and regulations provide that all food ingredients introduced into interstate commerce in the United States must be free of poisonous or deleterious substances that may be injurious to health; may not contain filth, undeclared ingredients, or otherwise be adulterated or unfit for food; must be prepared, packed, and held under sanitary conditions whereby the food will not become contaminated or rendered injurious to health; must be properly labeled; and must include or provide only ingredients that are "generally recognized as safe" ("GRAS") for use, or that are food additives or color additives that have been approved as safe by the FDA.

Terminations

All terminations of employment, for whatever reason, must be reviewed and cleared by the Legal Department prior to execution.

Trade Associations and Charitable, Educational, and Standard Setting Organizations

In accordance with the Conflict of Interest Policy and Antitrust Policy, no Employee may accept an appointment as a member of a trade association or charitable, educational, or standard setting organization without prior written approval by the Legal Department (***See* Conflicts of Interest Policy, Antitrust Policy, and Request for Approval to Serve on Other Boards**).

Waivers

Waivers or exceptions to the Code will be granted by the General Counsel 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.



Sensient Technologies Corporation

Code of Conduct Appendices

Appendices

I. Antitrust Compliance Policy

II. Company Confidential Information Policy

III. Conflict of Interest Policy

IV. Director and SAC Confidentiality Policy

V. Insider Trading Policy

VI. Anti-Bribery Policy

VII. Records Retention Policy

VIII. Supplier Code of Conduct

IX. Administration and Forms

SENSIENT®



Sensient Technologies Corporation

Antitrust Compliance Policy

To All Sensient Employees:

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

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

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

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

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

Sincerely,

Paul Manning

Chairman, President, and Chief Executive Officer



Introduction

Antitrust laws aim to promote and preserve competition among companies by outlawing actions that unreasonably restrict competition. [10] The justification for these laws is that free competition promotes consumer welfare by leading to lower prices, higher quality products and services, and more innovation. On the other hand, restrictions on competition can lead to higher prices, lower quality, and less innovation, all of which hurt consumers.

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

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

and

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

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

Any Employee with information about an actual or potential violation of antitrust law must immediately contact the Legal Department at 414-347-3777 or make an anonymous report using Sensient's Concerns Form located on Sensus. Employees who do report actual or potential violations are protected from retaliation by the Sensient Code of Conduct.

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



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

Dealings with Competitors

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

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

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

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

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

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

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

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

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

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



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

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

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

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

Dealings with Customers, Suppliers, and Distributors

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

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

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

Examples of competitive restrictions that require Legal Department consultation include: [11]

- Setting minimum resale prices for distributors or resellers;
- Customer, territorial, and other non-pricing restrictions on distributors or resellers;
- Tying and bundling arrangements; [12]
- Exclusive dealing and requirements/output contracts; [13] and
- For commodities products, charging different prices to similarly situated customers.



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

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

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

Market Power

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

Having market power means that we have the long-term power to raise prices and exclude competitors. Quantitatively speaking, market power generally means that sales of our product represent 50% or more of the sales in the relevant product or geographic market [14] The question of when or if we have market power in the relevant product or geographic market is extremely complex.

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

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

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

Always consult with the Legal Department concerning these issues.

[14] In the EU (as well as the United States, depending on which party occupies the White House), the threshold for market power can be as low as a 35% market share.

Other Prohibited Practices

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

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

Accordingly, these practices are all prohibited by this Policy.

Mergers And Acquisitions and Joint Ventures

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

Consequences Of Antitrust Violations

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

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

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

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

SENSIENT®

Sensient Technologies Corporation

Company Confidential Information Policy



Company Confidential Information Policy

The Company must protect its trade secrets and confidential information (collectively, "Company Confidential Information") so it can succeed as a business. Those who steal, 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 almost all countries, trade secrets are protected by law. 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.

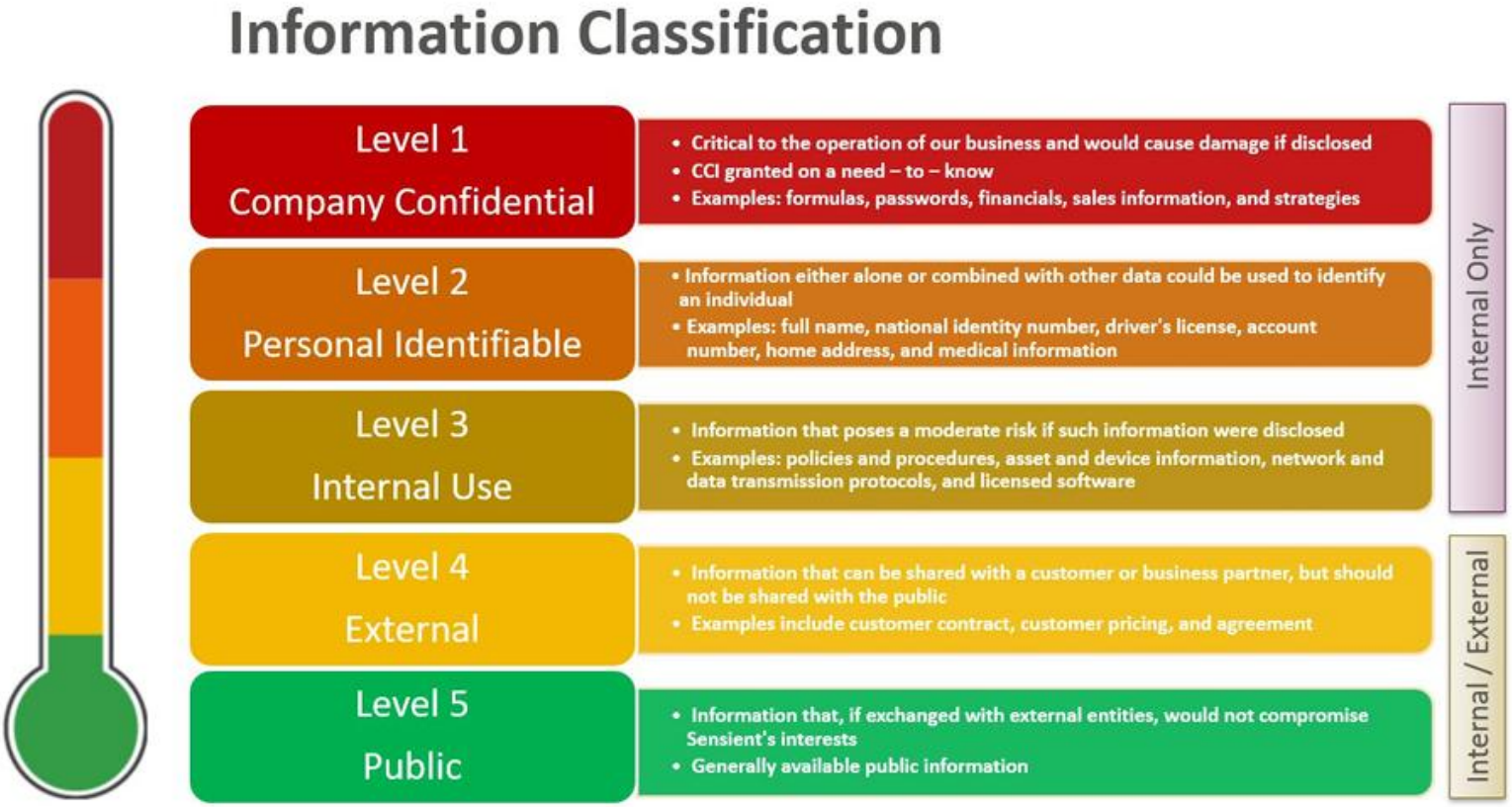
Confidential information is other non-public, sensitive information which may not fall within the legal definition of "trade secret," but is nonetheless valuable because it is not known by others and efforts are made to protect it. Confidential information includes all non-public information that, if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

It is the Company's policy to keep certain aspects of the business affairs of the Company and our customers confidential to the greatest possible extent. If, during the course of your employment, you acquire or have access to confidential or proprietary information about the Company and customers, except as otherwise provided by law, such information is to be handled in strict confidence per the terms of the agreement. Your failure to honor this confidentiality requirement may result in disciplinary action, up to and including termination.

While you work for Sensient, as well as after you leave, you cannot take, use, or disclose any CCI without the Company's permission. Employees must also sign a written agreement (which may be part of a written employment agreement) agreeing to protect CCI both during and after employment with the Company; however, the failure to sign such agreement will not relieve them of the duty to follow the obligations set forth in the Code of Conduct.

Sensient Classification System

The Company classifies all electronic information, including emails, Word documents, Excel files, PowerPoint presentations, and other paper and electronic files using the following designations:



Proper Handling Sensitive Information:

- Properly mark all documents, emails, presentations, and other files with the appropriate classification.

- Access to CCI is 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.

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

- Employees may only use CCI on the Company's Electronic Communications System (ECS). Employees may not place CCI on any non-Company device.

- Employees may not disclose CCI to non-employees without a signed non-disclosure agreement approved by the Legal Department.

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

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

- Upon leaving the Company, or at the Company's request, an Employee must immediately return all CCI in his or her possession.

Other Employee Responsibilities:

- DO NOT allow anyone else to use your system privileges;
- DO NOT share your usernames or passwords with anyone else;
- DO NOT exceed your authorized access;
- DO NOT copy or transmit CCI to a non-Company computer system, external drive (e.g., thumb drive, USB); non-Sensient email or website (e.g., Drop Box, Gmail, or any unapproved Artificial Intelligence system).
- DO secure your usernames and passwords to prevent unauthorized use;
- DO properly log out of systems when they have completed use; and
- DO shred or permanently delete all CCI that is no longer needed.

IT Department Responsibilities

The Corporate IT Department will implement technologies and controls to prevent unauthorized access and use of the Company's computer systems and CCI.

- Access to CCI will be controlled using a secure means of authentication, such as by use of passwords to confirm correct association with a username or account name.
- Once computer access to relevant CCI is established, appropriate security mechanisms will prohibit an individual user from exceeding his or her authorized access.
- CCI contained on designated high risk IT systems may not be removed, downloaded, or exported from such high-risk IT systems without prior authorization from the Chief Information Officer.
- The Chief Information Officer has the authority to designate high risk IT systems and to notify all users of such designations.
- When a new Employee reports for duty or there is a change in job responsibilities, his or her immediate supervisor will determine the Employee's need for a user account and the level of access required for the performance of the Employee's job.
- The supervisor will then send an appropriate request for such authorization and access to the Senior Manager for approval.
- Upon approval by the Senior Manager, the Employee's supervisor will send the approved request to the person in the Corporate or local IT Department charged with creating user accounts.
- Each Employee must use all mandated cybersecurity technologies and controls; any misuse or circumvention of these technologies or controls is a violation of the Code.
- Train Employees annually.
- Work with Corporate Security to ensure the physical security of IT systems.

Internal Audit Department Responsibilities

- Audit compliance with this policy as part of its regular audits.

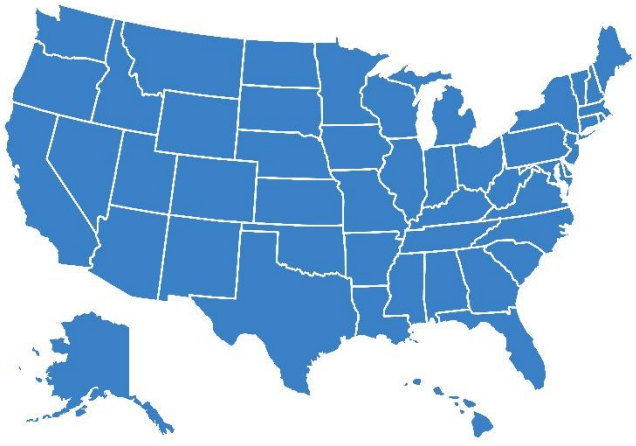


Special Notes for U.S. Employees

Nothing in this Policy prohibits Employees from: (1) reporting possible violations of federal or state law or regulation to, or participating in investigations by, any governmental agency or entity, including but not limited to the U.S. Department of Justice, the Securities and Exchange Commission, the National Labor Relations Board, the Congress, and any agency Inspector General; (2) making other disclosures that are protected under the whistleblower provisions of federal or state laws or regulations; or (3) for Employees protected by the National Labor Relations Act, exercising any Section 7 rights that they may have to communicate about working conditions.

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

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





Sensient Technologies Corporation

Conflicts of Interest Policy

Conflict of Interest Policy

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

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

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

- **Interest in Entities Transacting Business with the Company.** Employees may not have a financial interest in a supplier, competitor, or customer of the Company. This includes, but is not limited to, ownership by an Employee or any member of his or her family of more than 5% of the stock either directly or indirectly in any outside concern that does business with the Company, except where such interest consists of securities of a publicly owned corporation and such securities are traded on the open market (unless such investments are of such a size as to have influence or control over the corporation). Employees will not have an interest in or perform any services for a supplier or customer of the Company except for owning a small minority interest in securities of a publicly owned company.
- **Gifts, Meals, and Entertainment.** A Sensient Employee may not accept from any individual or company providing or proposing to provide goods or services to the Company any (i) cash, (ii) gift worth more than $50USD, (iii) hospitality or entertainment worth more than $100USD, or (iv) loans (other than from established banking or financial institutions). The gift and hospitality/entertainment dollar limits are the limits for a single calendar year for gifts and hospitality/entertainment from a single vendor. On a case-by-case basis and with the approval of one's Group President (as applicable), an Employee may make a written request for a waiver to these limits to the General Counsel.

- **Loans**. The Company will not extend, maintain, or arrange for any personal loan to or for any director or officer unless (1) there are extraordinary circumstances; (2) the loan is approved by the Board of Directors; and (3) all required disclosures are made under SEC and NYSE rules and regulations.

- **Use of Company Assets.** Employees are responsible for ensuring that corporate assets are used only for valid corporate purposes. Company assets include our equipment, inventory, corporate funds, and office supplies. They also include our concepts, business strategies and plans, confidential information, trade secrets, financial data, intellectual property rights, and other information about our business. These assets may not be improperly used to provide personal gain for Employees or others.
- **Company opportunity.** Employees owe a duty to the Company to advance its legitimate interests when the opportunity to do so arises. Employees are prohibited from (i) taking personal advantage of opportunities that are discovered through the use of corporate property, information, and position, (ii) using corporate property, information, or position for personal gain, and (iii) competing with the Company. Employees will not buy or sell for themselves or their family any security or property interest which they know the Company may be considering buying or selling until the Company has publicly announced its decision regarding the transaction and has concluded its interest in the subject.
- **Transactions.** Employees will not compete with the Company directly or indirectly in the purchase or sale of property or products without full disclosure to the Legal Department.
- **Conflicting roles.** Employees cannot represent the Company in any transaction in which the Employee or any family member or close friend has a substantial interest. For example, if an Employee engaging a vendor has any familial relationship (applying the definition of "Family Member" below) or close friendship with the vendor there is a conflict of interest. Accordingly, such conflicted Employee must disclose that relationship to his or her supervisor and may not control the selection of such vendor. If such vendor is nonetheless selected after an appropriate review by non-conflicted Employees, the conflicted Employee may not be the final approver for any invoice from such vendor.
- **Employment of Family Members.** Although Employee referrals, including referrals of family members, provide a valuable pipeline of talent for the Company, the simultaneous employment of members of the same family (as defined below) can give rise to actual or perceived conflicts of interest. Accordingly, prior approval for hiring a family member must be obtained as follows:

Family member of any current Employee	General Manager, unless conflicted
Family member of GM, Group President/Vice President, or Group Director	VP, Human Resources
Family member of CEO, CFO, or other Corporate Vice President or Senior Vice President	Board of Directors

"Family member," for purposes of this requirement, includes a spouse, domestic partner, parent, stepparent, child, stepchild, sibling, half-sibling, stepsibling, grandparent, grandchild, aunt, uncle, niece, nephew, first cousin, parent-in-law, child-in-law, sibling-in-law, or any individual residing in the employee's household or with whom the employee has a familial relationship that could create an actual or perceived conflict of interest.

- **Employment outside the Company.** Employees will not accept employment outside the Company that adversely affects the manner in which an Employee performs duties or fulfills responsibilities to the Company, or which violates the terms of any contract between the Employee and 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 Legal Department (***See* Request for Approval to Serve on Other Boards**). 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 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 Legal Department so that they can help make that determination.



Sensient Technologies Corporation

Director and SAC Confidentiality Policy

Director and SAC 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 and members of the Scientific Advisory Committee who are not directors ("SAC members") may not disclose Confidential Information (as defined below) unless they first obtain the express permission of the Board.

Accordingly:



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

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

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

Sensient Technologies: Level 4 External



Sensient Technologies Corporation

Insider Trading Policy

Insider Trading Policy

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

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

In addition, the Company itself shall not repurchase any shares of the Company's stock while in possession of material nonpublic information unless pursuant to a valid Rule 10b5-1 plan. Before engaging in repurchases or adopting a Rule 10b5-1 plan, management must give careful consideration as to whether or not the Company is in possession of material nonpublic information. While the risk of the Company possessing material nonpublic information is generally lower if a repurchase occurs during an open trading window, management must conduct this evaluation in all cases.

In accordance with Section 3(d) of the Company's Share Repurchase Policy, Sensient's internal Disclosure Committee shall meet before the corporation: (i) repurchases any shares, unless pursuant to a valid Rule 10b5-1 plan, or (ii) adopts a Rule 10b5-1 plan, in each case to determine whether the corporation is in possession of material nonpublic information or otherwise should refrain from repurchasing shares at such time pursuant to applicable securities laws.

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

What Information is "Material"?

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

Examples of some types of material information include:

- Financial results or financial forecasts for the quarter or the year;
- A major change in management or personnel;
- Possible mergers, acquisitions, joint ventures, and investments in other companies;
- Changes in relationships with significant customers;
- The gain or loss of an important contract, customer, or supplier;
- Actual or suspected cybersecurity risks or incidents, including vulnerabilities and breaches;
- Important product developments;
- Governmental approval of major new products;
- Major financing developments; or
- Major litigation developments.

While these examples illustrate the types of information that would likely be considered material, the list is not complete. Questions regarding or any uncertainty whatsoever concerning what sorts of information are material that are 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. However, any change in election or other reallocation of funds involving Company stock under an employee benefit plan is subject to the Company's prohibitions against illegal insider trading and cannot be completed while in possession of material nonpublic information (and, for officers, must be completed in a window period).

Trading in Other Securities

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

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

Consequences of Illegal Insider Trading

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

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

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

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

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

Restrictions on Legal Insider Trading

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

Window Periods

To limit the risk that Employees inadvertently violate insider trading laws, Employees are only permitted to trade Company stock during quarterly "window periods." All Employees are strongly advised to contact the Legal Department before buying or selling Company stock.

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

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

Event-Specific Blackout Periods

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

Because the very existence of a blackout period could signal to investors that a material event is pending, the Company will not announce, internally or publicly, that a blackout period is in effect; instead, the Legal Department will notify any officer, director, or other

Employee that knows of the material event and who seeks pre-clearance to trade during a blackout period on an individual basis that a blackout period is in effect. No person made aware of a blackout period should disclose the existence of the blackout period to any other individual.

Trade Pre-Clearance for Directors, Officers, General Managers, Business Unit Directors, Senior Financial Officers & other Employees

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

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

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

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

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

Immediate Reporting of Trades by Directors and Officers

Federal insider trading laws require the reporting of transactions by officers and directors on a timely basis. Therefore, it is Company policy that once a transaction has been executed on behalf of an officer or director, that officer or director must

immediately notify the General Counsel, by both telephone and e-mail, of the terms of the transaction. All reports will be retained for no less than five years.

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

Additional Trading Prohibitions

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

Rule 10b5-1 Trading Plans

Directors and officers who have entered into Rule 10b5-1 trading plans approved by the Company's board of directors need not adhere to the above requirements in the Code of Conduct regarding trade pre-clearance for directors and officers, window periods, or blackout periods with respect to trades occurring in compliance with the board-approved Rule 10b5-1 plan. However, directors and officers continue to have an obligation to follow the immediate reporting requirements outlined above. Any director or officer that enters into a Rule 10b5-1 trading plan will also need to comply with applicable securities laws, including: (i) mandatory cooling-off periods, (ii) restrictions on multiple overlapping plans and single-trade arrangements, (iii) relevant certifications, and (iv) acting in good faith.





Sensient Technologies Corporation

Anti-Bribery Policy

Sensient Technologies Anti-Bribery Policy

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

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

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

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

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

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

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



Foreign Corrupt Practices Act (FCPA) Overview

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

The books and records provisions require covered companies to make and keep accurate books and records; to devise and maintain an adequate system of internal accounting controls; and to prohibit knowingly falsifying books and records or knowingly circumventing or failing to implement a system of internal controls. The books and records provisions apply to bribery of foreign officials as well as to commercial bribery.

The FCPA applies to every Employee of Sensient regardless of where they work. 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 a $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 $26,262; for a books and records violation, the range is $11,823 up to $236,451 for individuals and $118,225 up to $1,182,251 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.

A Sensient director, officer, or employee may not accept from any individual or company providing or proposing to provide goods or services to the Company any (i) cash, (ii) gift worth more than $50USD, (iii) hospitality or entertainment worth more than $100USD, or (iv) loans (other than from established banking or financial institutions). The gift and hospitality/entertainment dollar limits are the limits for a single calendar year for gifts and hospitality/entertainment from a single vendor. On a case-by-case basis and with the approval of one's Group President (as applicable), a director, officer, or employee may make a written request for a waiver to these limits to the General Counsel.

Permitted Payments

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

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

Facilitating or Expediting Payments

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

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

Example: *The Company cannot pay an immigration official to expedite the processing of immigration paperwork for a new employee.*

Example: *The Company cannot pay a customs official to speed up the inspection process for the Company's products*.

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

Gifts, Travel, and Entertainment Expenses

For Foreign Officials and U.S. Government Officials

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

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

Example: *A Company officer or employee may never give a gift to any employee of a company owned in whole or part, or controlled by a foreign government, regardless of the occasion, local practice, or local law.*

Example: *A Company officer or employee may not pay the restaurant bill for a dinner with a customs official or an employee of a company owned in whole or part or controlled by a foreign government.*

Example: *A Company officer may not pay or offer to pay the travel expenses of an officer of a state owned enterprise who wants to visit one of our facilities.*

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

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

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

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

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

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

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

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

For Non-Governmental Customers and Business Partners

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

On limited occasions, with prior approval of the responsible General Manager, an officer or employee may give a gift to or pay for the cost of a meal or other entertainment expense for, an officer or employee of a non-governmental customer or business partner. The value for a gift must be less than $100 USD (per person), and the value of the meal or entertainment expense must be less than $500 USD, unless the General Counsel pre-approves a greater amount in writing. The gift cannot consist of cash or a cash equivalent (example: gift card). The gift should be given openly and transparently; provided only to reflect esteem or gratitude; permitted under local law and custom; and reasonable for the occasion. For meal and entertainment expenses, the Sensient officer or employee should be in attendance and pay the cost directly to the restaurant or entertainment venue.

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

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

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

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

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

Charitable Donations

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

Political Donations

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

Due Diligence for Third-Party Business Partners that Interface with Foreign Officials on Behalf of Sensient

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

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

Because of the risks involved, Sensient will 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/her designee will endeavor to conduct due diligence in accordance with these principles:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Watch For Warning Signs

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

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

- They were specifically recommended by a foreign official.

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

- They provide incomplete, inaccurate, or inconsistent disclosures.

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

- They request a "success fee."

- They request reimbursement for poorly documented or questionable payments.

- They request false or inaccurate invoices or documentation.

- They make unusually large or frequent political contributions.
- They have family or business ties to a relevant foreign official.
- Their only business qualification is influence over, or connection to, a foreign official.

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

Mergers and Acquisitions

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

Annual Training

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

Annual Certification

Each director, officer, and employee must sign an annual acknowledgement and reaffirmation of their responsibilities under the policy (*See* Appendix B (Employees) or Appendix B (Third Parties), as applicable). Each third-party business partner (who interfaces with a foreign government official on behalf of Sensient) must sign such acknowledgement and reaffirmation every three years after first signing such acknowledgement. Each President and General Manager will send these certifications to the Legal Department.

Contact Report Requirement

All Sensient directors, officers, and Employees must report to the 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 Legal Department.

Reports Of Violations of this Policy

Reports of violations or suspected violations of this policy must promptly be made to one's supervisor, an appropriate officer of the relevant subsidiary, or the General Counsel. The Code of Conduct provisions regarding Reporting Possible Violations will apply in all respects. No employee will be penalized for making a report in good faith.

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

Audits

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

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

Anti-Bribery Compliance Officer

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

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

Reports to the Audit Committee

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

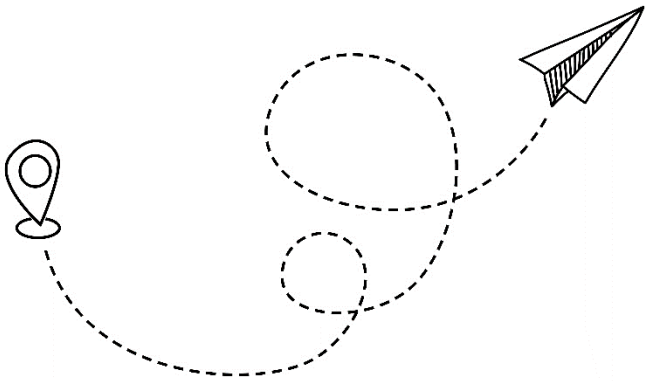
Investigations

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

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

Records Retention

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





Sensient Technologies Corporation

Anti-Bribery Policy Appendices

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.

Has the Company been provided with a copy of Sensient's anti-bribery policy?

____ yes ____ no

Does the Company have 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 Legal Department: _____

Pledge to Abide by Sensient's Anti-Bribery Policy and Anti-Bribery Laws

Name: _____

Title: _____

Business Unit: _____

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

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

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

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

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

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

I understand that if I have any questions about Sensient's Anti-Bribery Policy, I may rely upon Sensient's 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 may never offer, provide, attempt to provide, nor authorize or cause anyone else to provide, anything of value to any government official.

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

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

_____

Signature/Date

APPENDIX C

Internal Audit Department Anti-Bribery Policy Checklist for Internal Audits

General

- Is the Sensient Anti-Bribery Policy posted in a conspicuous place in the facility?
- Has every employee signed an acknowledgement and reaffirmation of their responsibilities under this Policy?

TPBP-Gs

- Can the entity's leadership identify all third-party business partners who interact with the government on behalf of the entity (TPBP-G)?
- Has due diligence been conducted on each TPBP-G?
    - Review copy of completed anti-bribery questionnaire for each TPBP-G.
    - Is each questionnaire current (required every three years)?
    - Are there any red flags present in any completed questionnaire?
    - Has the person who interfaces with the TPBP-G observed any red flag behavior by the TPBP-G?
- Does the entity have a signed Anti-Bribery Pledge from each TPBP-G?
    - Is the pledge current? (required annually)
- Where permitted, does the entity pay legitimate government fees (taxes, customs duties, licensing fees, etc.) directly to the responsible government agency rather than through a TPBP-G?
    - If the entity is legally authorized to make direct payments, but does not, what is the justification?
    - Are legitimate payments by a TPBP-G to a government agency documented in the TPBP-G's invoice(s) and in the entity's books and records?

- Are payments made to the TPBP-G for its services reasonable and in line with market prices (i.e., not above market price, padded, or steeply discounted)?
    - Ensure that we do not pay a third-party business partner in cash, nor make payments into offshore accounts or in any other non-standard or unconventional manner.

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

State Owned Enterprises

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

- Does the entity properly treat SOEs as government entities?

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

Gifts

- Has the entity presented, or been requested to present, any gifts to any government official or SOE employee? (If yes, immediately report this to the General Counsel)
    - Was the gift properly documented in the books and records of the entity?

- Has the entity presented any gifts to any commercial business partner?
    - Was each gift properly documented in the books and records of the entity?

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

- Was any gift a cash gift?
    - If yes, does entity have documentation of prior, written approval from the General Counsel? (If no, immediately report this to the General Counsel)

Meals, Entertainment, and Travel Expenses

- Has the entity paid, or been requested to pay, for any meal, entertainment, or travel expense for any government official or SOE employee? (If yes, immediately report this to the General Counsel)
    - Was each meal, entertainment, or travel expense properly documented in the books and records of the entity?

- Spot check books and records entries for routine meal, entertainment, or travel expenses paid for commercial business partners.
    - For meal and entertainment expenses over $500 USD, does the entity have documentation of prior, written approval from the General Counsel?

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

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

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

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

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

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

The Sensient Anti-Bribery Policy

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

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

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

SENSIENT®

Sensient Technologies Corporation

Records Retention Policy



Records Retention Policy

Reasons for this Policy

Proper management and retention of our corporate records is critically important. Various laws require Sensient and its subsidiaries to maintain particular records, usually for specific time periods. The accidental or intentional destruction of these records could result in fines and penalties, loss of rights, criminal and civil sanctions (for both individuals and the corporation), and serious damage to our ability to defend ourselves in litigation.

Sensient must retain certain records because they contain information that has enduring business value and/or must be kept in order to meet legal, accounting, and other regulatory requirements. This policy is part of a company-wide system for the review, retention, and destruction of records Sensient creates or receives in connection with the business it conducts. This policy also complies with the Sarbanes-Oxley Act, under which it is a crime to change, conceal, falsify, or destroy any record with the intent to impede or obstruct any official or government proceeding.

Employees are prohibited from inappropriately destroying any records, files, documents, samples, and other forms of information covered by this policy.

Types of Documents Covered by this Policy

This policy explains the differences among Records (as defined below), disposable information, and confidential information belonging to others.

Records

This policy covers any information created, received, or transmitted while conducting Sensient's business, regardless of physical format (“Record”). Such information may be located in computer programs, contracts, electronic files, e-mails, invoices, letters and other correspondence, memory in cell phones and PDAs, performance reviews, and test samples.

Any paper Records and electronic files that are part of any of the categories listed in the Records Retention Schedule must be retained for the amount of time indicated in the Records Retention Schedule.

A record must not be retained beyond the period indicated in the Records Retention Schedule, unless a valid business reason, litigation hold, or other special situation requires its continued retention. If you are unsure whether to retain a certain record, contact a member of the Legal Department.

Disposable Information

Disposable information consists of data that may be discarded or deleted at the discretion of the user once it has served its temporary useful purpose. It consists of data that may be safely destroyed because it is not a Record as defined by this policy. Examples may include:

- Duplicates of originals that have not been annotated.
- Preliminary drafts of letters, memoranda, reports, worksheets, and informal notes that do not represent significant steps or decisions in the preparation of an official record.
- Books, periodicals, manuals, training binders, and other printed materials obtained from sources outside of Sensient and retained primarily for reference purposes.
- Spam and junk mail.

Confidential Information Belonging to Others

As provided by the Company Confidential Information Policy in the Code of Conduct, confidential information that an Employee obtained from a source outside of Sensient, such as a previous employer, must not, so long as such information remains confidential, be disclosed to or used by Sensient. Unsolicited confidential information submitted to Sensient should be refused, returned to the sender where possible, and deleted, if received via the internet.

Mandatory Compliance

Responsibility of All Employees

Sensient strives to comply with all applicable laws, rules, and regulations as well as with recognized compliance best practices. Employees must comply with this policy, the Records Retention Schedule, and any litigation hold communications. Failure to do so may subject Sensient, its Employees, and its contractors to serious civil and/or criminal liability. An Employee's failure to comply with this policy may result in disciplinary sanctions, including termination.

Reporting Policy Violations

Sensient is committed to enforcing this policy as it applies to all forms of Records. The effectiveness of Sensient's efforts, however, depends on Employees. If you feel that you or someone else may have violated this policy, you should report the incident immediately to your supervisor. If you are not comfortable bringing the matter up with your immediate supervisor, or do not believe the supervisor has dealt with the matter properly, you should raise the matter with a member of the Legal Department or through Sensient's Concerns Form on Sensus or Voice Mailbox (*See* Reporting Possible Violations). If Employees do not report inappropriate conduct, Sensient may not become aware of a possible violation of this policy and may not be able to take appropriate corrective action. No one will be subject to, and Sensient prohibits, any form of discipline, reprisal, intimidation, or retaliation for reporting incidents of inappropriate conduct of any kind, pursuing any record destruction claim, or cooperating in related investigations.

Legal Department's Responsibilities

The Legal Department is responsible for identifying the documents that Sensient must or should retain and determining the proper period of retention. It also arranges for the proper storage and retrieval of Records, the destruction of Records whose retention period has expired, and coordination with outside vendors where appropriate. Additionally, the Legal Department will:

- Administer the document management program and help department heads implement it and related best practices.
- Advise Employees on how to comply with this policy.
- Periodically review the Records Retention Schedule and administrative rules issued by various U.S. and non-U.S. government agencies to determine if Sensient's document management program and its Records Retention Schedule is in compliance with state and foreign regulations.
- Distribute from time to time to the various department heads information concerning applicable laws and administrative rules relating to Records.
- Ensure that the maintenance, storage, anonymization, and destruction of Records is carried out in accordance with this policy, the procedures of the document management program, Sensient's Global Privacy Policy, and the requirements of applicable law (including the European Union's General Data Protection Regulations and the California Consumer Privacy Act).

- Evaluate the overall effectiveness of the document management program.
- Review periodically the implementation of the document management program in each of Sensient's departments and correct any noncompliance with this policy.

How to Store and Destroy Records

Storage

Sensient's Records must be stored in a safe, secure, and accessible manner. Any documents and financial files that are essential to Sensient's business operations during an emergency must be duplicated and/or backed up at least once per week and maintained off site.

Destruction

The Legal Department is responsible for the continuing process of identifying Records that have met the required retention period and supervise their destruction. The destruction of confidential, financial, and personnel-related Records must be conducted by shredding if possible. Non-confidential Records may be destroyed by recycling. The destruction of electronic Records must be coordinated with the IT Department. The destruction of Records must stop immediately upon notification from the Legal Department that a litigation hold is to begin because Sensient may be involved in a lawsuit or an official investigation (see next paragraph). Destruction may begin again once the Legal Department lifts the relevant litigation hold.

Litigation Holds and Other Special Situations

Sensient requires Employees to fully comply with its published Records Retention Schedule and procedures as provided in this policy. Employees should note the following general exception to any stated destruction schedule: If you believe, or the Legal Department informs you, that Sensient Records are relevant to current litigation, potential litigation (that is, a dispute that could result in litigation), government investigation, audit, or other event, you must preserve and not delete, dispose, destroy, or change those Records, including e-mails, until the Legal Department determines those Records are no longer needed. This exception, usually referred to as litigation hold or legal hold, replaces any previously or subsequently established destruction schedule for those Records. If you believe this exception may apply or have any question regarding whether it may apply, please contact the Legal Department.

A litigation hold may also require the retention of information not normally retained under this policy. Because litigation often takes many years to resolve, litigation holds may likewise be in place for many years.

In addition, you may be asked to suspend any routine document disposal procedures in connection with certain other types of events, such as the merger of Sensient with another organization or the replacement of Sensient's IT systems.

Internal Review and Employee Questions

Internal Review

The Legal Department will periodically review this policy and its procedures with legal counsel and/or certified public accountants to ensure Sensient is in full compliance with relevant new or amended regulations.

Questions About this Policy

Any questions about this policy should be referred to a member of the Legal Department.

Conflicts with Sensient’s Privacy Policy or the Requirements of Applicable Law

In the event of a conflict between this policy and Sensient’s privacy policy or the requirements of applicable law (including the European Union’s General Data Protection Regulation), the terms set out in Sensient’s privacy policy or the requirements of applicable law will prevail.

Records Retention Schedule

Occasionally Sensient establishes retention or destruction schedules or procedures for specific categories of records. This is done to ensure legal compliance and accomplish other objectives, such as protecting intellectual property and controlling costs. Employees should give special consideration to the categories of documents listed in the record retention schedule below. Avoid retaining a record if there is no business reason for doing so and consult with a member of the legal department if unsure.

Record	Retention Period
1. **Personal Records**	
Benefits descriptions per employee	Duration of employment + 4 years
Collective bargaining agreements	Duration of agreement + 3 years
EEO-1 Reports	Filed annually, most recent kept on file
Employee applications and resumes	1 year from date of submission for applicants not hired, duration of employment + 1 year for employees
Employee benefit plans subject to ERISA (includes plans regarding health and dental insurance, 401K, long-term disability, and Form 5500)	6 years from when the record was required to be disclosed
Employee offer letters (and other documentation regarding hiring, promotion, demotion, transfer, lay-off, termination, or selection for training)	1 year from date of making record or action involved, whichever is later, or 1 year from date of involuntary termination

Sensient Technologies: Level 4 External

Records relating to background checks on employees	6 years from when the background check is conducted
Employment contracts; employment and termination agreements	Duration of agreement + 3 years
Employee exposure records (e.g., industrial hygiene monitoring results, material safety data sheets) and employee medical records	Duration of employment + 30 years
Employee records with information on pay rate or weekly compensation	Duration of employment + 3 years
I-9 Forms	3 years after date of hire or duration of employment + 1 year, whichever is later
Occupational injury/illness records (e.g., OSHA Forms 300, 300A, and 301)	5 years following the end of the calendar year that these records cover
Job descriptions, performance goals, and reviews; garnishment records	Duration of employment + 2 years
Employee polygraph test records	3 years from when the test is conducted
Employee tax records	4 years from the date tax is due or paid
Medical exams required by law	Duration of employment + 30 years
Pension plan and retirement records	Permanent
Pre-employment tests and test results	1 year from date of personnel action
Salary schedules; ranges for each job description	2 years following the end of the calendar year that these records cover

Time reports	Duration of employment + 3 years
Training agreements, summaries of applicants' qualifications, job criteria, interview records, and identification of minority and female applicants	Duration of training + 4 years
Workers' compensation records	Duration of employment + 30 years
Written affirmative action program (AAP) and supporting documents	For immediately preceding AAP year, unless it was not then covered by the AAP year

Payroll Records

Payroll registers (gross and net)	3 years from the last date of entry
Federal procurement contract and related weekly payroll documents	4 years from completion of contract
Time cards; piece work tickets; wage rate tables; pay rates; work and time schedules; earnings records; records of additions to or deductions from wages; records on which wage computations are based	2 years following the end of the calendar year that these records cover
W-2 and W-4 Forms and Statements	As long as the document is in effect + 4 years

Corporate Records

Articles of Incorporation, Bylaws, Corporate Sea	Permanent
Annual corporate filings and reports to secretary of state and attorney general	Permanent

Board policies, resolutions, meeting minutes, and committee meeting minutes	Permanent
Contracts	Duration of agreement + 7 years
Construction documents	Permanent
Documents relating to corporate mergers, acquisitions, the sale or purchase of stock or assets, or other similar events	Permanent
E-mails (business related)	3 years following the end of the calendar year that these records cover
Fixed Asset Records	Permanent
IRS Form 1023 (Application for charitable and/or tax-exempt status)	Permanent
IRS Determination Letters	Permanent
Manufacturing batch records	3 years following the end of the calendar year that these records cover
Sales and purchase records	3 years following the end of the calendar year that these records cover
State sales tax exemption documents	Permanent
Resolutions	Permanent

SEC Records	
Documents supporting management's assessment of internal controls over financial reporting	Permanent
Press releases and public filings	Permanent
Original signature pages or other documents showing the signatures of certifying officers in SEC filings	5 years from date of filing
Records relevant to an SEC audit or review, including memoranda, correspondence, and other communications	5 years after conclusion of audit or review
Internal Audit	
Internal audit reports	7 years after conclusion of internal audit
Supporting documents and work papers relevant to an internal audit	5 years after conclusion of internal audit
Accounting and Finance	
Accounts Payable and Receivables ledgers and schedules	7 years following the end of the calendar year that these records cover
Annual audit reports and financial statement	Permanent
Annual plans and budgets	2 years following the end of the calendar year that these records cover
Bank statements, cancelled checks, deposit slips	7 years following the end of the calendar year that these records cover
Business expense records	7 years following the end of the calendar year that these records cover

Cash receipts	4 years following the end of the calendar year that these records cover
Electronic fund transfer documents	7 years following the end of the calendar year that these records cover
Employee expense reports	7 years following the end of the calendar year that these records cover
General ledgers	Permanent
Journal entries	7 years following the end of the calendar year that these records cover
Invoices	7 years following the end of the calendar year that these records cover
Petty cash vouchers	3 years following the end of the calendar year that these records cover
Tax Records	
Annual tax filings, tax returns (income, franchise, and property), tax bills, tax receipts, tax statements, and all supporting work papers	Permanent
Filings of fees paid to professionals (IRS Form 1099 in the US)	7 years from date of filing
Payroll tax withholdings	7 years following the end of the calendar year that these records cover
Earnings records	7 years following the end of the calendar year that these records cover
Payroll tax returns	7 years from date of filing
State unemployment tax records	Permanent

Legal and Insurance Records	
Appraisals	Permanent
Copyright registrations	Permanent
Documents related to actual, potential, or threatened litigation, government investigation, audit, or other similar event	7 years after later of the conclusion of litigation, investigation, audit, or other similar event, or the event(s) underlying any of the foregoing
Environmental studies of owned or leased properties (e.g., Phase I/II Environmental Site Assessments, groundwater/soil sampling data, environmental remediation records, etc.)	Permanent
Insurance claims applications	Permanent
Insurance disbursements and denials	Permanent
Insurance contracts and policies (Director and Officers, General Liability, Property, Workers' Compensation)	Permanent
Judicial or administrative consent documents	Permanent
Leases	Duration of agreement + 6 years
Patents, patent applications, and supporting documents	Permanent
Real estate documents (including loan and mortgage contracts, deeds)	Permanent
Stock and bond records	Permanent
Trademark registrations, evidence of use documents	Permanent
Warranties	Duration of warranty +7 years

Environmental Compliance Records	
Environmental permits	Permanent
Environmental compliance records, including any records required to be created or maintained by any environmental permit (e.g., waste water sampling data, air emission test reports, etc.)	5 years following the end of the calendar year that these records cover
Hazardous waste manifests	Permanent
Asbestos and lead-based paint survey records	Life of building

SENSIENT®



Sensient Technologies Corporation

Supplier Code of Conduct

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

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

Failure to comply with this Supplier Code of Conduct may be grounds for terminating the supplier relationship, and any relevant contracts, depending on the seriousness of the violation. Material violations, including but not limited to forced labor, child labor, bribery, human trafficking, and trade regulations and sanctions violations will result in immediate termination of the supplier relationship.

Business Practices

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

Compliance With All Applicable Laws and Regulations

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

Antitrust and Fair Competition

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

No Bribery or Corrupt Payments

Sensient has a comprehensive Anti-Bribery Policy that requires behaviors that exceed the requirements of the United States Foreign Corrupt Practices Act and the United Kingdom Bribery Act as well as most local laws. Under these laws, suppliers are prohibited from corruptly paying, offering to pay, or authorizing the payment of, money or anything of value, directly or indirectly, to a foreign official in order to influence any official action or decision, or to obtain a business advantage. A “foreign official” is anyone who exercises governmental authority at the local, state, or national level, and may include directors, officers, or employees of state-owned enterprises. Our suppliers must comply with these laws as well as our Anti-Bribery Policy while working on our behalf and be equally vigilant against bribery and corruption risks within their own organizations.

Intellectual Property

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

Cybersecurity

Suppliers will implement all necessary measures, and review them regularly, to protect their computer systems and networks. They will put in place appropriate controls to identify and mitigate relevant cybersecurity risks. Suppliers will notify Sensient within 24 hours of becoming aware of a known or suspected data breach of its or its suppliers’ systems and/or networks that may impact Sensient. Suppliers will work with Sensient and, if applicable, law enforcement to contain and respond to such breach.

Protection of Confidential Information and Personal Information

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

Artificial Intelligence

To the extent suppliers use artificial intelligence (“AI”) in conducting business with Sensient, Sensient requires suppliers to uphold standards of transparency, data protection, and ethics and to comply with all applicable laws and regulations governing or related to the use of AI. Sensient also requires suppliers to provide clear information

to Sensient on how AI is used, what data is collected, how it is processed, and how/where it is stored. No Sensient data may be input to any AI system without prior written consent from Sensient. Sensient retains all rights in its data including any intellectual property rights in any output derived from Sensient's data. Suppliers shall be responsible for, and shall indemnify Sensient against, any losses, claims, or damages arising from the supplier's use of AI in connection with goods or services provided to Sensient, including any intellectual property infringement claims related to AI-generated outputs.

Conflict of Interest

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

Gifts

Gifts to or from Sensient employees are neither expected nor necessary for business relationships between our supplier and Sensient. Our Code of Conduct prohibits Sensient employees from accepting from any individual or company providing or proposing to provide goods or services to the Company any (i) cash, (ii) gift worth more than $50USD, (iii) hospitality or entertainment worth more than $100USD, or (iv) loans (other than from established banking or financial institutions).

Affiliation with Governments and Government Officials

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

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

- Any officer or employee of a foreign government, regardless of rank;
- Employees of government-owned or government-controlled businesses;
- Foreign politicians, political parties, or candidates for office; and
- A family member or agent of the above.

Embargoes and Trade Law

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

Management and Transparency

Our suppliers are expected to have systems in place to track compliance with applicable laws and regulations and to investigate, to the extent allowed by law, allegations of

misconduct. Suppliers must immediately inform Sensient in writing if they are aware of any material noncompliance with local laws involving either the supplier or a Sensient product.

Supply Chain Due Diligence

Our suppliers are expected to regularly review the practices occurring within their supply chain to support the identification and management of potential risks and to ensure the maintenance of standards outlined in this document. Suppliers will work to ensure appropriate levels of accountability, including policy setting for suppliers (such as a supplier code of conduct detailing expectations) and compliance monitoring.

Responsible Sourcing

Our suppliers must disclose the country of origin for the primary materials for all deliveries made to Sensient. Sensient reserves the right to request a full supply chain map of our suppliers in order to facilitate risk assessments and gauge legal and ethical compliance in the upstream supply chain. Our suppliers will be transparent about all known facilities used to produce products or services for us and provide such information upon request. If requested, suppliers are expected to provide reports on the presence of substances in any materials supplied to Sensient that may be restricted by, or require disclosure to, governmental bodies, customers, and/or recyclers.

Conflict Minerals

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

Workforce Practices

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

Human Rights

Our suppliers must respect and support global human rights, in accordance with the principles found in the International Bill of Human Rights, the UN Guiding Principles on Business and Human Rights, and the ILO Declaration on Fundamental Principles and

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

No Forced Labor or Trafficking

Our suppliers are prohibited from using slaves or forced labor of any kind, including prison labor, non-rescindable contracts, indentureship, or labor obtained through threats of punishment, deposits of bonds or travel documents, or other constraints, or engaging in human trafficking. Suppliers will conform to Convention 29 (Forced Labour) and Convention 105 (Abolition of Forced Labour) of the International Labor Organization. If applicable, supplier is expected to have filed a transparency statement in compliance with the UK Modern Slavery Act 2015. All suppliers are required to abide by applicable forced labor laws, including the United States' Uyghur Forced Labor Prevention Act (UFLPA), as well as Sensient's Uyghur and Other Forced Labor Policy.

No Child Labor

Our suppliers are prohibited from employing children under the age of 15 years (or any higher age established by applicable law). Young employees within the ages of 15-18 years must never be exposed to work that is likely to harm their physical or mental health, safety, or morals. Adequate support must be provided to enable young employees to attend and complete compulsory education. Suppliers must have a remediation plan in place if child labor is identified that removes the child from unlawful work. Suppliers will conform to Convention 138 (Minimum Age) and Convention 182 (Worst Forms of Child Labor) of the International Labor Organization.

No Harassment or Abuse

Our suppliers are prohibited from harassing or abusing employees. Our suppliers must treat their employees with respect and dignity, and without harassment or abuse of any kind. To the extent permitted by law, suppliers must strive to provide a workplace free of any form of harassment, intimidation, or victimization, whether physical, psychological, or sexual.

Nondiscrimination

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

Diversity and Inclusion

Our suppliers are expected to value the dignity of each employee as a unique person with individual skills and perspectives. Suppliers are expected to categorically reject

individuals and ideologies that seek to sow hate, discord, and division based upon an individual's personal characteristics. Suppliers should strive to unite themselves with their employees by focusing on their common humanity and by dedicating themselves to the principles of integrity, professionalism, and safety.

Reasonable Compensation

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

Working Hours, Overtime, and Wages

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

Worker Recruitment

Suppliers must provide prospective employees with accurate details of working conditions in the host location, including worker's legal rights, the nature of work, wages, benefits, and the duration of contract at the time of recruitment, in a language the prospective employees understand.

Workplace Health and Safety

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

Respect the Right of Workers to Freely Organize, Associate, and Bargain Collectively in Accordance with Applicable National Laws

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

Environmental Practices

Our suppliers must treat the environment with respect, including:

Environmental Compliance

At a minimum, our suppliers will conduct their businesses in compliance with all applicable laws in a way that minimizes impact to the environment. As practical,

suppliers should seek to reduce their environmental impact beyond what the law currently requires.

Environmental Management System

Our suppliers should design and implement processes to assess risks, set targets, and implement action plans for reducing environmental impacts, including but not limited to greenhouse gas emissions, water consumption and conservation, waste, wastewater, energy efficiency, air, water and soil pollution, use of chemicals, the protection of biodiversity, and, where applicable, responsible agriculture practices.

Hazardous Waste Management

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

Air Quality and Carbon Footprint

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

Energy Efficiency

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

Water Management and Conservation

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

No Deforestation

Our suppliers will take appropriate steps to ensure their actions avoid negative impacts on forests, peatlands, and other protected areas. When establishing new operations or expanding existing ones, our suppliers shall obtain all legal approvals and permissions. We also expect our suppliers to keep documentary evidence of land use history and provide it if requested. We expect our suppliers to act consistently with the European Union Deforestation Regulation and other laws and regulations that require supply chain transparency documentation.

Community Practices

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

Property Rights

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

Free, Prior, and Informed Consent (FPIC)

Our suppliers commit to following the principles of free, prior, and informed consent (FPIC) of indigenous peoples for property or land negotiations and require the same commitment from their suppliers and sub-contractors. All forms of land grabbing are prohibited. Adherence to the principles of free, prior, and informed consent of indigenous peoples is required in all negotiations for property or land, including the use of and transfers of it. Land rights of individuals, indigenous people, and local communities affected by sourcing practices, supply chains, and operations are respected.

Human Right to Water

Our suppliers acknowledge that every human being has the right to safe, clean, affordable, and accessible water adequate for human consumption, cooking, and sanitary purposes.

Health and Safety Impact

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

Indigenous People

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

Local Sourcing

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

Continuous Improvement

Our suppliers must continuously improve their operations and methods.

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

If there is a grievance brought against a supplier by stakeholders or otherwise brought to our attention, we may initiate an investigation by our Legal Department. We will review any report of non-compliance made in good faith. A member of our Legal Department may conduct outreach to the supplier to discuss any concerns or findings. The supplier shall assist with any such review and provide access to any information reasonably requested.

If remediation is required, the supplier will be expected to implement a corrective action plan to effectively and promptly resolve the failure and keep us informed of its progress.

Violation Reporting

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

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

If at any time a supplier or one of its employees or contractors believes that there has been a violation of the Sensient Supplier Code of Conduct, the supplier or its employee is encouraged to report its concerns to our Compliance Hotline at 1-414-347-3897 or supplierconcerns@sensient.com.

Declaration Of Compliance

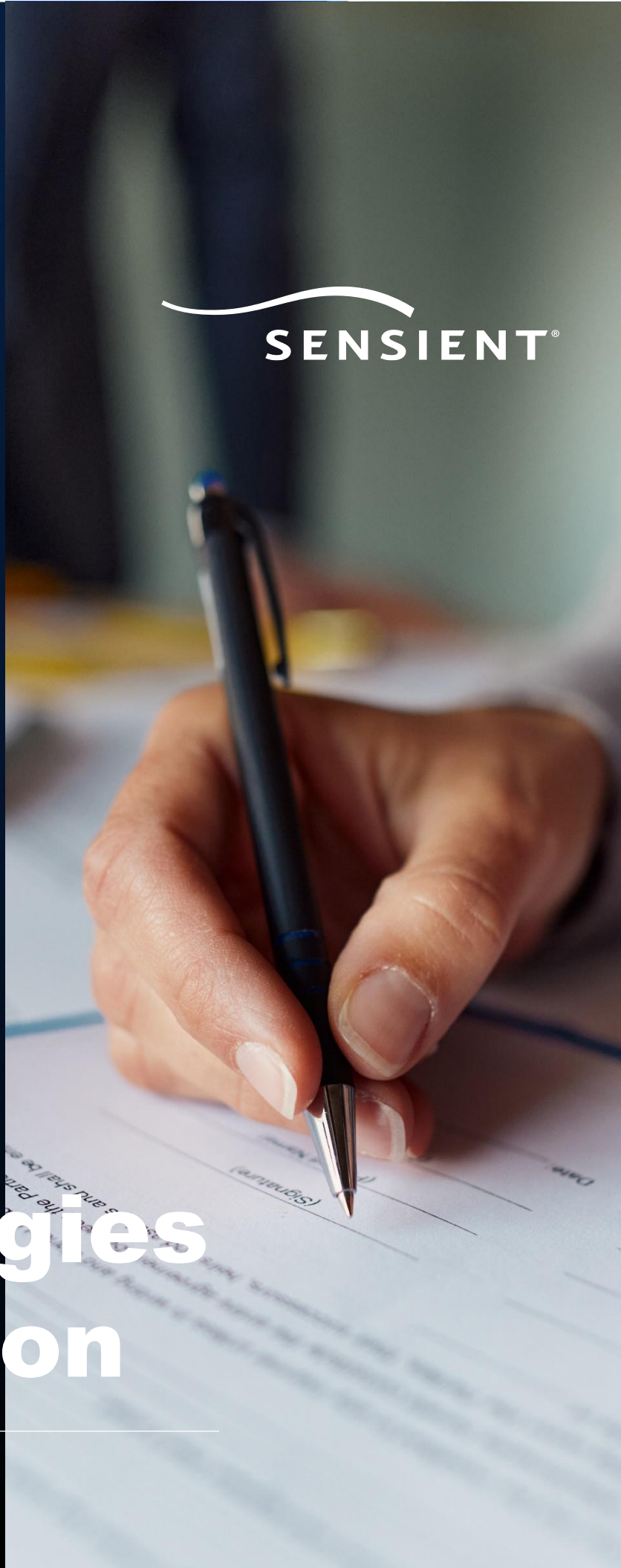
Supplier declares the following:

- Supplier has read and understands the Sensient Supplier Code of Conduct (Update 2025).
- Supplier agrees to comply with the principles embodied in the Sensient Supplier Code of Conduct (Update 2025) while working with Sensient.
- Supplier agrees that Sensient reserves the right to terminate any agreement or business relationship with any supplier that cannot demonstrate substantial compliance with the principles embodied in this Supplier Code of Conduct.
- Supplier undertakes to improve or correct any identified deficiencies. Where applicable, Sensient may require corrective action and the implementation of continuous improvement plans as a condition of doing business.
- Supplier agrees that Sensient reserves the right to assess and/or monitor compliance with the principles embodied in this Code, where applicable through a third-party, and to do so in any way deemed necessary (reasonable on-site inspections, questionnaires, interviews, etc.).
- Supplier agrees to conduct due diligence throughout its supply chain on its employees, agents, subcontractors, suppliers, and sub-suppliers to the extent they are involved in the provision of goods and/or services to Sensient to ensure substantial compliance with the principles embodied in this Supplier Code and applicable law.

On behalf of Supplier:

Title _____ **Date** _____

Sensient Technologies: Level 4 External



Sensient Technologies Corporation

Administration

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

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

The 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 as well as to relevant individuals and entities that perform work for or on behalf of the Company. 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.

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

Monitoring Compliance

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

Periodic internal audits will be conducted throughout the Company by the Internal Audit Department in conjunction with the 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.

Sensient Technologies Corporation

Request for Approval to Serve on Other Boards

To: General Counsel, 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: _____

Sensient Technologies: Level 4 External

Initial Employment Statement

Sensient Technologies Corporation
Code of Conduct
Statement and Questionnaire

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

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

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

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

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

Stock Date of Purchase: _____

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

Organization Ownership Interest Date of Purchase: _____

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

Relationship Date of Commencement: _____

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

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

_____

Employee Signature

_____

Position Department Location

_____

Date

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

Sensient Technologies Corporation
Code of Conduct
Certificate

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

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

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

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

_____

Signature

_____

Print name

_____

Position Department Location

_____

Date

_____

Supervisor/Witness

_____

Date

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: _____