



CODE OF BUSINESS CONDUCT AND ETHICS

May 2023

SUMMARY OF THE CODE'S PRINCIPLES

PROTECTING THE COMPANY'S ASSETS, RESOURCES AND DATA

- We often have sensitive confidential information about Scantime, other companies, our Clients and investors, and our directors, officers and employees; preserving the integrity of this information is vital to our business and reputation and is necessary to meet our obligations under data protection laws.
- Electronic communications relating to business activities may not be conducted through electronic communication systems that have not been specifically approved for business activities, including (among others) personal email accounts, personal text messaging, nonapproved chat forums, and social media.

ACCURACY OF BOOKS AND RECORDS AND PUBLIC DISCLOSURES

- We should take care that our books and records are accurate and that all of our business transactions are properly authorized.
- As a public company, we have duties to our shareholders and must ensure that our communications and other disclosures to the market are true and accurate.

DUTIES TO STAKEHOLDERS

In asset management, one's reputation is everything and we should act responsibly in dealings with our securityholders, customers, Clients, investors, suppliers, other stakeholders and competitors.

- We have obligations to our Clients and must manage their capital as though it were our own.

COMMUNICATIONS AND MEDIA

- In this digital era, be careful in your written communications made over company information systems, such as email, as this is a permanent record.
- You must ensure that your online activities, including your use of social media, are appropriate and reflect well on Scantime Energy.

CONFLICTS OF INTEREST AND PERSONAL BEHAVIOR

- Scantime will be a global brand and as a representative of the company your personal behavior must be consistent with our values.
- As a steward of third-party capital, be cognizant that you face a heightened risk that your personal interests may conflict with or appear to conflict with the interests of the company.

POSITIVE WORK ENVIRONMENT

- We value diversity and we should all do our part to maintain a respectful work environment where everyone feels safe, included and productive.
- Our success is dependent on establishing a workplace culture free from discrimination, violence, harassment and other negative influences.

COMPLIANCE WITH LAWS, RULES, REGULATIONS AND POLICIES

- We operate in many jurisdictions and are subject to different laws, rules and regulations; you need to be aware of the laws that apply to your activities so that you can comply with them; ignorance of the law is no excuse.
- The company has corporate policies that you must be familiar with, as they govern your trading activities, business practices and other conduct while at Scantime.

FREQUENTLY ASKED QUESTIONS

WHY DO WE HAVE A CODE?

The Code serves as a guide for how you should conduct yourself as a member of the Scantime team. Preserving our corporate culture and ensuring compliance with legal, regulatory and fiduciary duties is vital to the organization and following the Code helps us do that.

WHO MUST FOLLOW THE CODE?

You have two responsibilities. First, you must follow every aspect of the Code and certify your commitment each year. Second, if you suspect someone may be violating the Code or the policies referred to herein, you have an obligation to report it. To make a report, follow the section of the Code: "Reporting Potential Code Violations."

WHAT ARE YOUR RESPONSIBILITIES?

You have two responsibilities. First, you must follow every aspect of the Code and certify your commitment each year. Second, if you suspect someone may be violating the Code or the policies referred to herein, you have an obligation to report it. To make a report, follow the section of the Code: "Reporting Potential Code Violations."

HOW WILL I KNOW IF THERE IS A PROBLEM?

The Code attempts to deal with the most common issues that you may encounter, but it cannot address every question that may arise. When you're not sure what to do, ask yourself the following questions:

- Is it illegal?
- Does it feel like the wrong thing to do?
- Would you feel uncomfortable if others knew about it?
- Will it have the potential to create a negative perception of you or the company?
- Do you have a personal interest that has the potential to conflict with the company's interest?

If you answer "yes" to any of these questions your proposed conduct may violate the Code and you should ask for help.

HOW SHOULD I ASK FOR HELP?

If you have questions about the Code, any policies or guidelines referred to herein, or about the best course of action to take in a particular situation, you should seek guidance from your supervisor or a member of Scantime's Legal & Regulatory Group

WHAT IF I WOULD LIKE TO MAKE AN ANONYMOUS REPORT?

. If you choose to make an anonymous report, your anonymity will be protected to the fullest extent possible as permitted by law. Keep in mind, however, that maintaining your anonymity may limit the company's ability to investigate your concerns.

WHAT ARE THE CONSEQUENCES FOR VIOLATING THE CODE?

Violations of the Code or the policies and guidelines incorporated by reference herein, can vary in its consequences. If you're an employee, it could result in a reprimand or other disciplinary action, including the termination of your employment at the company for cause. If you're a director, a violation may necessitate your resignation. Certain violations of the Code also contravene applicable laws and therefore can have severe consequences outside of Scantime. Depending on your actions, failing to comply with the Code could lead to civil or criminal prosecution, which could result in substantial fines, penalties and/or imprisonment.

STANDARDS OF BUSINESS CONDUCT

Scantime seeks to foster and maintain a reputation for honesty, openness, trust, integrity and professionalism. The confidence and trust placed in Scantime by our Clients and investors is something we value greatly and endeavor to protect. In many respects, our reputation is our most vital business asset. Accordingly, all our activities should be conducted with honesty and integrity and in compliance with applicable legal and regulatory requirements. We have adopted the Code and related policies and procedures to preserve our culture and to ensure compliance with legal, regulatory and fiduciary requirements applicable to our activities. We expect and require that you meet the letter and spirit of the Code (and related policies and procedures). This Code incorporates by reference the following corporate policies and programs which should be read in conjunction with the Code:

- Advisory Records Retention Policy;
- Anti-Bribery and Corruption Policy;
- Vendor Management Program;
- Anti-Modern Slavery and Human Trafficking Policy;
- Data Protection Policy and Data Protection Program;
- Disclosure Policy;
- Enterprise Information Security Policy;
- Personal Trading Policy;
- Positive Work Environment Policy;
- Signing Authority and Approval Thresholds Policy;
- Travel and Entertainment Expense Policy;
- Regional Political Contributions Policies; and • Whistleblowing Policy.

PROTECTING THE COMPANY'S ASSETS, RESOURCES AND DATA

The company's assets are to be used for legitimate business purposes only.

The company's assets are for business, not personal use. The company's assets span many categories. Assets can be physical, tangible goods, such as office supplies, furniture, computers or intangible items, such as intellectual property.

You have a responsibility to safeguard the company's assets from loss, damage, theft, misuse and waste. If you become aware of loss, damage, theft, misuse or waste of our assets, or have questions about your proper use of them, you should speak with your supervisor. The company's name (including its corporate letterhead and logo), facilities and relationships are valuable assets and must only be used for authorized company business.

If you use the company's assets for personal benefit or are otherwise wasteful with the company's assets, you may be in breach of your duty to the company. You have a responsibility not to abuse company resources for reimbursement. Any requests for reimbursement for authorized company expenses must be for legitimate business expenses. If you are unsure whether a certain expense is legitimate, you should speak with your supervisor or refer to the company's Travel and Entertainment Expense Policy.

Confidential information must be protected at all times.

We must protect confidential information in our possession both information about us and information about other companies, and our Clients and investors. Confidential information includes, but is not limited to, material non-public information, all confidential memos, notes, lists, records and other documents in your possession, in hard and soft copy.

All of these are to be delivered to the company promptly after your employment ceases or at any time upon the company's request, and your obligation to protect this information continues after you leave the company. You must protect hard and soft copies of confidential information that are removed from the office (e.g., to be worked with at home or at external meetings).

It is important to use discretion when discussing company business. This includes respecting information barrier protocols and discussing company business only with those individuals at the company that have a "need to know" the information. Additionally, be careful not to discuss company business in public places such as elevators, restaurants, and public transportation or when using your phone or email outside of the office. You should also be careful not to leave confidential information in unattended conference rooms or in public places where others can access it. While at Scantime, if you become aware of confidential information about the company or another entity that you know or suspect has been inadvertently disclosed, seek guidance from a member of the Legal & Regulatory Group before using or acting upon this information.

Personal data held by or on behalf of the company must be used in compliance with data protection laws.

The company collects personal data regarding individuals both inside and outside the organization where we have the lawful basis for doing so. This is necessary to effectively and efficiently administer and manage the operation of our business. Personal data includes, among other things, sensitive personal, medical and financial information. We should take all reasonable steps to only hold personal data for as long as we have a need to retain it.

Collection and use of personal data are subject to various legal and regulatory requirements. You must take all reasonable steps to ensure that personal data is kept confidential and accessed only by those individuals at the company that have a need to know this information to carry out their duties. In addition, if it is necessary to the conduct of business to disclose personal data to a third-party (e.g., so that a third-party may provide services to the company or acquire an asset or business of the company) then you must ensure that such transfer complies with applicable legal and regulatory requirements. This may include ensuring the third-party is subject to a written agreement which contains confidentiality obligations and, where relevant, other obligations which must be included under the data protection laws of certain jurisdictions in which we operate or have Clients or investors. In all other cases, you may only disclose personal data pursuant to a legal or regulatory requirement.

In addition, you should ensure that the personal data is protected in a manner that is consistent with how personal data is protected by the company within these jurisdictions, and in any event in compliance with all applicable data protection laws.

You are responsible for ensuring that you understand and comply with our data protection/privacy policies. For more information about compliance with data protection laws, refer to the company's Data Protection Policy and related policies referred to in the Data Protection Program

Intellectual property belongs to the company.

During the course of your employment, you may be involved in the creation, development or invention of intellectual property such as concepts, methods, processes, inventions, confidential information and trade secrets, know-how, physical products, ideas, plans, programs, software, applications, code, works of authorship, trademarks, service marks and designs, alone or jointly with others, including but not limited to the improvement of existing intellectual property belonging to the company.

All such intellectual property and the rights therein shall be owned by the company and your moral rights to such intellectual property, if any, will be waived. You are responsible for cooperating with the company and providing all necessary assistance, including the preparation and execution of any necessary documentation such as assignments and applications to register rights before relevant government authorities on behalf of the company, to ensure that all intellectual property and related rights become or are recognized as the exclusive property of the company.

The documents of the company must be preserved.

It is critical that you help preserve our business records, follow the guidelines set forth in any document retention policies and comply with related legal and regulatory requirements. Investment Access Persons and Access Persons should refer to the company's Advisory Records Retention Policy for further details on the appropriate preservation of advisory records.

If you are notified that your documents are relevant to an anticipated or pending litigation, investigation or audit, you must follow the guidance set forth in the notification you receive from legal counsel regarding retention of documents.

ACCURACY OF BOOKS AND RECORDS AND PUBLIC DISCLOSURES

Ensure that the books and records of the company are complete and accurate and that all business transactions are properly authorized.

The books and records of the company must reflect all its transactions in order to permit the preparation of accurate financial statements. Employees must never conceal information from

- (i) an external auditor;
- (ii) an internal auditor; or
- (iii) an audit committee of the company.

In addition, it is unlawful for any person to fraudulently influence, coerce, manipulate or mislead an external auditor of the company. The company's contracts and agreements govern our business relationships. Because the laws governing contracts and agreements are numerous and complicated we have put in place policies and procedures to ensure that any contract entered into by the company has the appropriate level of approval.

As a result, employees who enter into contracts or agreements on behalf of the company must have proper authorization to do so and, prior to their execution, these documents must be reviewed by legal counsel where required by policy or practice. If you are unsure whether you have proper authorization to enter into a contract on behalf of the company, refer to the company's Signing Authority and Approval Thresholds Policy.

Ensure that the company provides full, true and plain public disclosure.

All employees who are responsible for the preparation of the company's public disclosures, or who provide information as part of this process, must ensure that public disclosures of information are made honestly and accurately.

Employees must be aware of and report any of the following:

- (a) fraud or deliberate errors in the preparation, maintenance, evaluation, review or audit of any financial statement or financial record;
- (b) deficiencies in, or noncompliance with, internal accounting controls;
- (c) misrepresentations or false statements in any public disclosure document, such as annual and quarterly reports, prospectuses, information/proxy circulars and press releases; or
- (d) deviations from full, true and plain reporting of the company's financial condition.

Additionally, each person who is in a financial reporting oversight role, and their Family Members, are prohibited from obtaining any tax or other services from the external auditor, irrespective of whether the company or such person pays for the services.

DUTIES TO STAKEHOLDERS

Deal fairly with the company's stakeholders.

You must deal fairly with the company's security holders, customers, Clients, suppliers, communities in which we operate, other stakeholders and competitors. To preserve our reputation and relationship with stakeholders, do not engage in any illegal or unethical conduct.

COMMUNICATIONS AND MEDIA

Use the company's various forms of communication properly and appropriately.

All business matters that involve electronic, written communication must be conducted by employees on the company's email system or through other systems provided and approved by the company. You must always use our e-mail, Internet, telephones and other forms of communication appropriately and professionally. Employees must comply with our Enterprise Information Security Policy and all related policies. While we appreciate the need for limited use of these tools for personal purposes, any such use should not be excessive or detract from your work.

As outlined in the summary of the Code's principles, electronic communications relating to business activities may not be conducted through electronic communications system that have not been specifically approved for business activities, including (among others) personal email accounts, personal text messaging, non-approved chat forums and social media.

Employees should not email business information to their personal email accounts or maintain a copy of business information on their personal computers or other non-work electronic devices. When using company-provided technologies, such as computers, cell phones and voicemail, you should not expect that the information you send or receive is private. Your activity may be monitored to ensure these resources are used appropriately and are in compliance with the company's policies and laws and regulations; please refer to the Employee Data Protection and Privacy Notice .

Be cautious in your use of social media.

The company's social media policy is that, unless you are expressly authorized, you are strictly prohibited from commenting, or posting about, or otherwise discussing the company, its customers and Clients, its (and its Clients') investors, its employees, and its securities, investments and other business matters on all social media forums, including, but not limited to, social networks, chat rooms, wikis, virtual worlds and blogs (collectively, "social media").

You are a representative of Scantime when engaging in online activities and you must ensure that your behavior online, including on social media, is appropriate and consistent with our values. For further details on the appropriate use of social media, you should refer to the company's Enterprise Information Security Policy.

Do not speak on behalf of the company unless authorized to do so.

If a shareholder, financial analyst, member of the media or other third-party contacts you to request information, even if the request is informal, do not respond to it unless you are authorized to do so. In this event, refer the request to your supervisor or forward the request to an individual at the company employed in investor relations or communications.

For further information, you should refer to the Disclosure Policy of Scantime or a Controlled Affiliate, as applicable.

CONFLICTS OF INTEREST AND PERSONAL BEHAVIOR

Exhibit personal behavior that reinforces a positive image of you and the company.

Your personal behavior, both inside and outside work, should reinforce a positive image of you, the company and its business activities. It is essential to use good judgment in all your personal and business dealings. You should refrain from engaging in activities that could hurt the company's reputation, or yours, and that could undermine the relationship of trust between you and the company or the company and its Clients.

Employees who have acted inappropriately may be subject to disciplinary action up to and including termination for cause.

Remember your duties to Scantime when participating in outside personal interests; obtain permission before pursuing business activities outside the scope of your role with the company

The company encourages directors and employees to be active participants in their community. While pursuing personal, political, not-for-profit activities or other like activities, be mindful that your participation in any outside interest must not prevent you from adequately discharging your duties to Scantime and should not conflict with or otherwise be adverse to the company's interests.

In addition, ensure that when you are involved in these activities you are not seen to be speaking or acting on behalf of the company without express authority.

Avoid situations in which your personal interests conflict with the interests of the company, its Clients or investors in Client accounts.

A "conflict of interest" for this purpose occurs when a person's private interest inclines the person, consciously or unconsciously, or appears to incline the person to act in a manner which is not in the interests of the company. You may have a conflict of interest if you are involved in any activity that prevents you from performing your duties to the company properly, or that may create a situation that could affect your ability to act objectively, effectively and in the best interests of the company, including due to among other things, personal interests or receipt of benefits from our relationships with companies, business partners, counterparties, investment banks, brokerage firms, service providers, and other constituencies.

Accordingly, you must place the company's interest in any business matter ahead of any personal interest. Remember that the company's interest includes the company's obligations to its Clients.

You may also have a conflict of interest or the appearance of a conflict of interest as a result of a "close personal relationship" with another employee at Scantime or a counterparty with which Scantime is engaging (e.g., a company employee's spouse works at an entity that is being considered as a service provider). To ensure that these relationships are managed appropriately, and to deal with any possible conflicts of interest in an appropriate and responsible manner, you are expected to disclose the existence of such relationships to your Human Resources ("HR") department.

For the purposes of the Code, a close personal relationship includes, but is not limited to, relationships with a parent or parent equivalent (e.g., adoptive parent), close relative or friend, spouse, fiancée, common law, or anyone else with whom you are in, or have been in, a romantic or intimate relationship.

The best way to judge whether you may have a conflict of interest is to ask yourself whether a well informed person would reasonably conclude that your interest, activity or close personal relationship could in any way influence your decision or performance in carrying out a duty on behalf of the company.

WAIVERS

A waiver of the Code will be granted only in very exceptional circumstances. A Code waiver for Scantime's employees, other than Scantime's executive officers, must be approved by the CEO. A Code waiver for Scantime's Board of Directors or executive officers must be approved by the Chair of the Board. A Code waiver for a director, officer or employee of a Controlled Affiliate may be granted in accordance with the policies of the Controlled Affiliate, as consistent with the Code.

AMENDMENTS

Scantime's Board of Directors reviews and approves the Code on at least an annual basis and is ultimately responsible for monitoring compliance with the Code.

LEGAL NOTICE

The company reserves the right to modify, suspend or revoke the Code and any related policies, procedures, and programs at any time. The company also reserves the right to interpret and amend the Code and these policies in its sole discretion.

Any amendments to the Code will be disclosed and reported as required by applicable law. The company employs unionized employees. If the Code conflicts with a collective bargaining agreement governing the wages and/or conditions of employment for unionized employees, the collective bargaining agreement will prevail; if a collective bargaining agreement is silent with respect to an area addressed in the Code, or if the Code supplements a collective bargaining agreement, unionized employees are expected to abide by the Code.

Neither the Code, nor any of the policies referred to herein, confer any rights, privileges or benefits on any employee, create an entitlement to continued employment at the company, establish conditions of employment for the employee, or create an express or implied contract of any kind between employees and the company. In addition, the Code does not modify the employment relationship between employees and the company.

The Code is posted on our website and intranet. The version of the Code on our website and intranet may be more current and supersedes any paper copies, should there be any discrepancy between paper copies and what is posted online.