DTCC

The home of **MarkitServ, Traiana, TriOptima** & **Reset**

Code of Conduct

2023

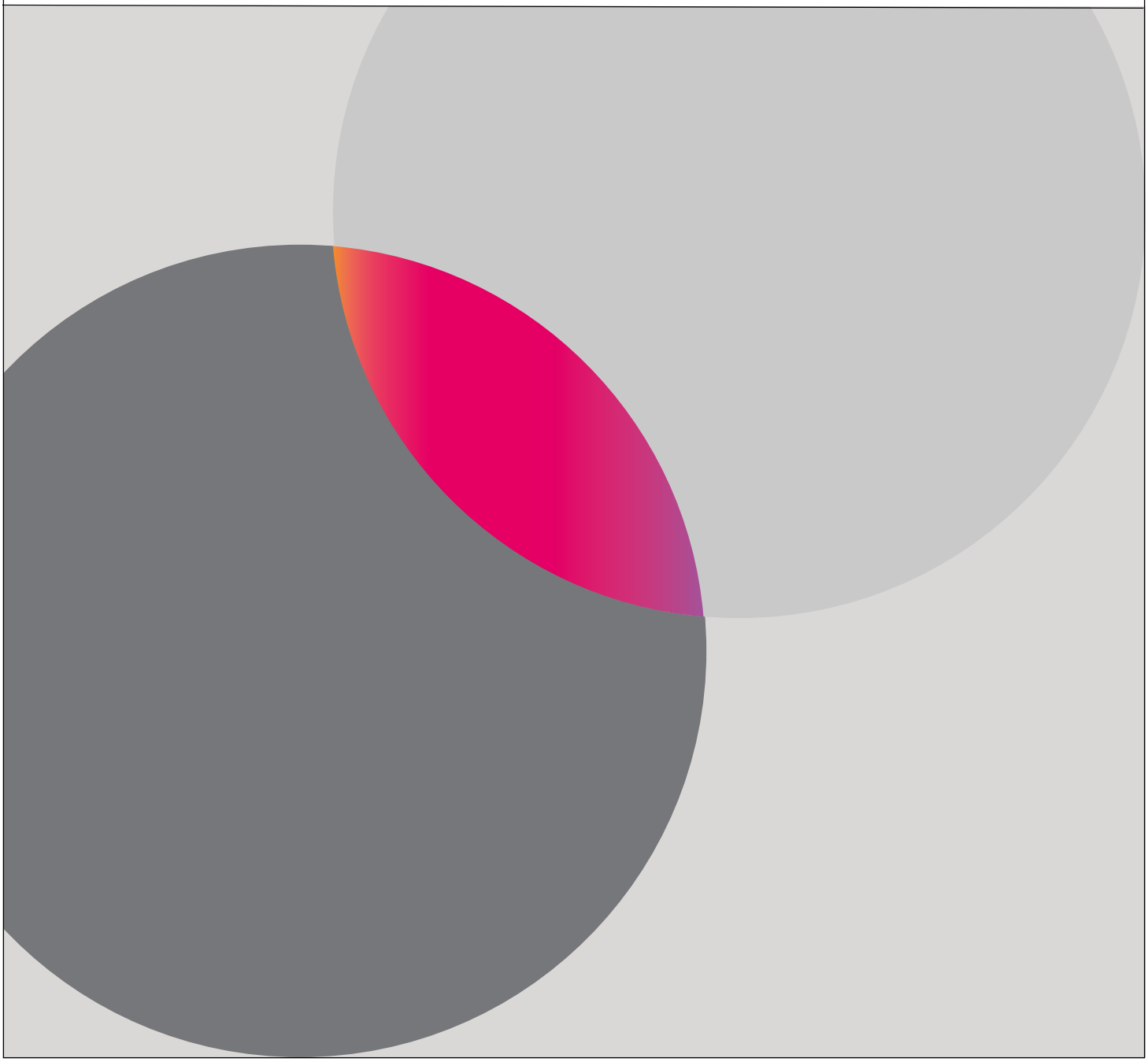


Table of contents

Letter from our Co-CEOs

Dear all,

At OSTTRA, we are proud of our reputation as a trusted leader within our industry. To achieve this, it is expected that every person within the firm commits to a set of ethical and responsible business practices that ensures we conduct our business with the highest levels of integrity.

Our Code of Conduct outlines our business standards and practices that we expect to hold ourselves to and reflects who we are and what we value as a firm. It's a commitment to our customers, shareholders, and each other that we will always operate with honesty, integrity, and respect.

As colleagues, we are all responsible for reading, understanding, and attesting to our Code of Conduct, which serves as a guide to empower us all to put our behaviours at the heart of the decisions we make and the actions we take.

Together, we can continue to build a culture of integrity and excellence that sets us apart in our industry.

Sincerely,

John and Guy

John Stewart and Guy Rowcliffe

OSTTRA

Understanding our code of conduct

Purpose of the Code

This Code of Conduct (Code) outlines what we stand for, our ethical standards and how we conduct business.

Our Code cannot cover every situation. For this reason, we have separate corporate policies, procedures and guidelines for our business practices that provide more detail and information. Even then, we cannot predict or plan for every scenario – so take a responsible and cautious approach, and where something seems wrong, even if it is not directly prohibited by a policy, please escalate, or refrain from acting.

Please refer to these additional materials, which we reference throughout the Code, to better understand our expectations and requirements. Abiding by legal requirements, ethical standards and this Code is critically important for all of us. Failure to do so could subject individuals and the company to fines and criminal penalties and could cause OSTTRA to lose its ability to conduct business around the world. It could also cause serious damage to our reputation. Keep in mind that there may be times when laws differ significantly from region-to-region.

If you find yourself in a situation where local law or custom conflicts with our Code or other company policies, please escalate this to our compliance team compliance@osttra.com to get further advice.

Application of the Code

Our Code applies to all employees, officers, and board members in all locations where we conduct business. We also expect our contractors, suppliers, and other business partners to comply with the law and ethical standards described in our Code, as well as the Third Party / Vendor Code of Conduct, which applies to all vendors, contingent workers and channel partners. You can find a link to our Third Party / Vendor Code of Conduct here.

Acting with integrity

Our behaviours

At OSTTRA we are guided by a set of behaviours that are designed to help us deliver against our strategic goals and drive forward our culture of ethics and integrity.

Some of these behaviours are to:

- Always look for ways to improve our systems, processes or how we do things
- Adopt an OSTTRA first mindset
- Champion and drive change
- Be prepared to challenge yourself and others
- Embrace a continuous learning mindset
- Take pride in the success of our customers
- Continually strengthen domain expertise and demonstrate it at all points of the customer lifecycle
- Strive for continued operational excellence

Equal opportunity employer

We have policies and processes in place to ensure we are an equal opportunity employer. This means our processes ensure equal employment opportunities without regard to race, colour, religion, sex, sexual orientation, gender identity or expression, national origin, age, disability, pregnancy, veteran status, genetic information, citizenship status or any other basis prohibited by applicable law.

We are committed to equal employment opportunities at all levels of our organisation.

This applies to all employment practices, including but not limited to, recruitment, hiring, employment, assignment, training, compensation, benefits, demotion or transfer, promotions, disciplinary action and terminations.

Diversity and inclusion

Diversity is reflected in our commitment to an inclusive workplace that values each individual and their unique contributions.

Our people are our most valuable asset. Their diverse characteristics, perspectives, ideas, and backgrounds give us a vital competitive edge.

We have high expectations for our people, which is to be:

- Respectful to each other
- A team who works together and embrace each other's diverse perspectives and backgrounds
- Aware and cognizant of our approach to work-life balance such as flexible work arrangements
- A work environment free from discrimination and harassment

Any inappropriate conduct or behaviour against others will not be tolerated. Any employee found to be acting in an inappropriate manner may be subject to disciplinary action, up to and including termination of employment.

Human rights

We are committed to responsible and transparent operations that demonstrate respect and support for all human rights.

This means:

- We will always treat our people and members of the communities where we do business with dignity and respect
- We will always conduct business in a legal, ethical and responsible manner
- We believe it is important to work with vendors who operate with the same high standards we set for ourselves

Safety and security in the workplace

We are committed to providing a safe and healthy workplace built on a foundation of strong and uncompromising ethics and integrity.

We all play an important role in creating that environment.

- We strive to create an environment where you can work in safety and comfort
- We maintain the security of our premises by safeguarding our people, physical assets, intellectual property, and other confidential, sensitive, and proprietary information
- We maintain a workplace safe and free from violence by prohibiting the possession or use of unauthorised dangerous weapons on company property

OSTTRA

Conflicts of interest

For any industry in which trust is a central feature, the need to have demonstrable standards of practice and the means to enforce them is a key requirement. We are committed to the highest level of integrity and complying with policies and controls relating to conflicts of interest.

A conflict of interest can be described as a situation in which someone in a position of trust has competing professional and/or personal interests that makes it difficult to fulfil their duties fairly.

While working at OSTTRA, you have an obligation to always do what is best for the company and its customers, above what would benefit you the most.

Conflicts of interest can arise between:
- OSTTRA and the interests of one or more customers
- Customers with competing interests
- Entities or individual functions or business divisions within OSTTRA
- You and the interests of one or more customers

There may be circumstances in which your personal interests could result in:
- A financial gain, or the avoidance of a financial loss, at the expense of a customer
- You have an interest in the outcome of a service provided to the customer in a transaction carried out on behalf of the customer, which is distinct from the customer's interest in that outcome
- You have a financial or other incentive to favour the interest of another customer or group of customers over the interest of the customer or potential customer
- You pursue or engage in the same kind of business as the customer or potential customer
- You receive (or expect to receive) inducements from a third party in relation to a service provided to the customer, in the form of monetary or non-monetary benefits or services

The list above is not exhaustive, and you have a responsibility to ensure that you adhere to our Conflicts of Interest policy.

The main question when assessing if such a conflict of interest exists is whether the customer may be put or perceived to be put in an unfavourable position.

You must avoid any type of conflict and identify any situations that create, or appear to create, a conflict between your personal interests, OSTTRA's interests and any customer's interests.

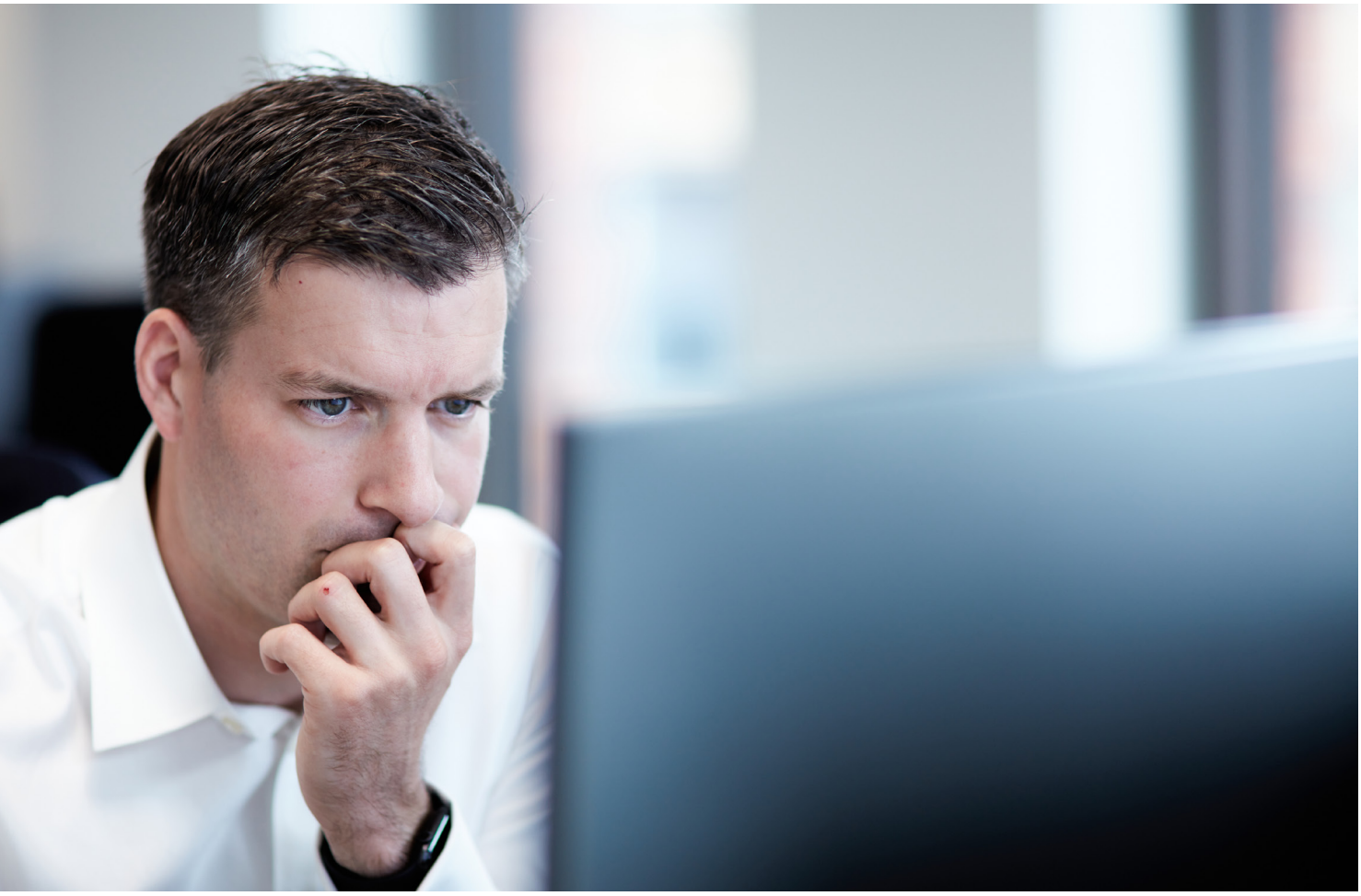
All potential conflicts of interest should be disclosed, via the S&P Global GECS system. It will be for your manager and our compliance team to decide if there is an actual conflict, and what, if any, adjustments need to be taken to remove the conflict.

Sustainability and corporate responsibility

Sustainability and corporate responsibility underpin our business and guide our corporate purpose to accelerate progress in the world by providing intelligence that is essential for companies, governments, and individuals.

Our strong commitment to driving progress begins with our own operations and value chain. We fulfil our environmental, social, and corporate governance (ESG) responsibilities as a company by creating a diverse and inclusive workplace, reducing our environmental footprint, upholding the highest standards of corporate governance, and actively engaging our suppliers to embrace our sustainability ambitions.

ESG considerations inform our corporate governance mechanisms for effective Board oversight as well as how we manage our company to fulfil our strategic priorities and carry out our corporate purpose to accelerate progress for stakeholders and communities across the world.



Gifts and entertainment

Developing relationships with our customers, vendors and other stakeholders is an important part of our business. Any giving or receiving of gifts, entertainment or other hospitality must be appropriate and reasonable, as well as in compliance with any legal requirements. In this way we will protect our reputation.

Gifts and entertainment should only be provided to strengthen business relationships and never with the aim to improperly influence the actions or decisions of another party. Improper gifts, entertainment, meals, or travel may create the appearance of a conflict – and where they are excessive, this may even risk appearing like a bribe.

Our Gifts and Entertainment Policy provides guidance on when it is appropriate to give or receive gifts or entertainment or other related hospitality, including the rules relating to government officials. Before accepting or providing any gift or entertainment, ensure you are familiar with the requirements of this policy.

The Annex to the Policy sets out limits that we see as reasonable, and not give a false perception of favouritism, bribery, or corruption.

Travel and entertainment

Expenses should be reasonable, directly related to company business and supported by appropriate documentation. If you travel or incur business-related expenses, you must be familiar with the requirements of the Travel, Entertainment and Expense Policy.

When submitting expenses, please make sure you have included the required documentation, you have clearly described the business reason for the expense, you have included the names and affiliations for all those who attended and have appropriately categorised the expense type.

If you are uncertain about whether something would be an appropriate expense, please contact your manager.

Managers are responsible for all money spent and expenses incurred by their direct reports and should carefully review all expenditures before providing their approval.

OSTTRA

Representing OSTTRA

To build our brand recognition, our experts around the world participate in media interviews and share commentary via social media platforms on a wide range of topics.

Our experts offer insight and analysis on news or thematic expertise pertaining to our industry. These interactions project the voice of OSTTRA, build our presence, promote recognition of our expertise and bolster our business and position in the marketplace.

Only those who have been granted permission to do so will be able to present the views of OSTTRA. If approached by media, or if you have a view that you would like expressed with the media please seek permission before answering or expressing the view.

This is to ensure that we give a consistent view across all aspects of the business. One view that is out of kilter with the rest of our media presence could jeopardise an important opportunity elsewhere.

Colleagues are expected to act with integrity and respectful to companies, shareholders and individuals.

For more information please refer to our Global Media Policy.

Communications with regulators and government agencies

Nothing in this Code of Conduct or any other OSTTRA policy prevents you from communicating directly with or providing non-privileged documents or other information to a regulator or government agency regarding possible violations of law. You may do so without disclosure to us and we may not retaliate against anyone for any of these actions.

In the course of your employment, it is unlikely that you will be contacted by or need to contact a regulator, policy maker, central bank, politician or government agency. Notwithstanding the above provision (concerning possible violations of law), you should consult with our compliance team mailto:compliance@osttra.com and / or with the head of legal, risk, compliance and government and regulatory affairs in the event of any such contact, either as soon as it has been received, or before you intend to reach out.

Treating customers fairly

As part of operating with the highest levels of integrity, we will treat our customers in an objective, even-handed and professional manner, taking care to avoid preferential treatment of one or more customers over others.

Any concerns or complaints raised by customers will be treated promptly, effectively and with respect. Communications with customers will be clear and in plain language that is easy to understand.

An issue will be classified as a complaint if there has been an oral or written expression of dissatisfaction, whether justified or not about the provision of an OSTTRA service.

Compliance with laws, rules and regulations

Anti-bribery and corruption

Bribery can be either active (offering, promising, or giving a bribe) or passive (requesting, agreeing to receive, or accepting a bribe). It makes no difference whether the person involved is a private person, a corporate entity, or a public official – what is relevant is whether there is an attempt, or a perception that there was an attempt to influence them with the intention of obtaining or retaining business.

Common indicators of bribery include:
- Payments for abnormal amounts or purposes
- Payments made in an unusual way
- Decisions are taken for which there is no clear rationale
- Records are incomplete or missing

We are committed to compliance with anti-bribery laws and regulations and will not give or receive illegal or improper payments, regardless of local business practices.

Decisions and actions concerning our businesses, and our relationships with third parties, will always be taken on objective grounds and without allowing any undue or improper influence.

We will follow our guiding principles and internal rules in the giving and receiving of gifts and entertainment.

Bribery and Corruption are criminal offences and could result in direct action against you and OSTTRA. We expect our vendors and other third-party relations to honour the same level of integrity and to exercise zero tolerance for bribery and corruption.

Money laundering and terrorist financing

We will not tolerate our services being used in connection with money laundering or terrorist financing and will take all reasonable steps to ensure that we do not receive or otherwise handle any funds that are the proceeds of a crime.

The methods by which money may be laundered are varied and can range in sophistication. Any involvement in a transaction or service that is designed to conceal or disguise the nature, location, source, ownership, or control of proceeds may constitute money laundering.

Money laundering is usually understood to be a three-stage process:

1. Placement - this means getting 'dirty' money into the financial system
2. Layering - this means mixing the 'dirty' money into the system so that it gradually 'disappears'
3. Integration - this is the result of placement and layering – the 'dirty' money is now indistinguishable from clean money and may be used

The following activities are prohibited by law and may additionally incur criminal sentencing, including up to 14 years imprisonment:

- Becoming involved in a money laundering scheme
- Failing to report a suspicion that a customer or a third party is engaged in money laundering
- "Tipping off" a person suspected of money laundering
- Destroying or disposing of documents related to an investigation
- Failing to produce information or providing misleading information in response to request for such information in an investigation of suspected money laundering

Comprehensive anti-money laundering procedures are in place to ensure that our customers are fully identified and that business purposes are properly understood.

This is known as 'Know Your Customer' (KYC) checks. All customers are subject to KYC and cannot be onboarded without up-to-date KYC. Red flags or other suspicions are escalated internally and are examined in order to determine the proper course of action, including external reporting where necessary.

If you have any reason to suspect that a customer or other third party has engaged in money laundering or terrorist financing, you must immediately notify the relevant designated Anti-Money Laundering Reporting Officer (MLRO).

Training is also provided to ensure sound awareness of internal anti-money laundering procedures as well as money laundering risks and typologies.

Please refer to our AML guidelines for more on your reporting obligations and the AML Rules

Sanctions

We comply with all applicable sanctions regimes including those that prohibit business or financial relationships with certain entities, industries, or regions. Customers are also routinely screened to ensure that necessary actions are taken in the event of any new or updated sanctions.

OSTTRA

Market abuse

For more information, please see the S&P Global Financial Crime Policy. The financial services industry is highly regulated and there are widespread laws and prohibitions against insider trading and other forms of market abuse.

Rules to be aware of include:

- Insider dealing and unlawful disclosure - The insider dealing rule prohibits persons in possession of inside information from using that knowledge to deal or attempt to deal in financial instruments or to recommend or induce another person to transact on the basis of inside information. Unlawful disclosure of inside information is where a person possesses inside information and discloses that information to any other person, except where the disclosure is made in the normal exercise of employment, a profession, or duties
- Market Manipulation – entering into a transaction, placing an order to carry out an execution or any other behaviour which gives or is likely to give false or misleading signals

You have an ethical and legal obligation to maintain the confidentiality of information about OSTTRA and the companies with which we do business.

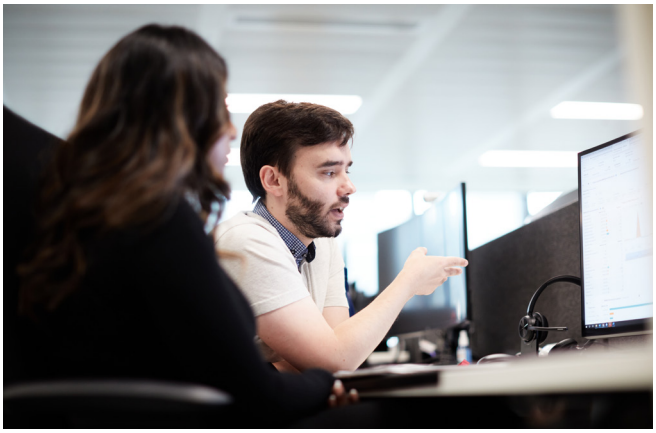
For more information on your obligations regarding market abuse and personal trading, please refer to our Market Abuse Policy and our Personal Account Dealing Policy.

Fraud

OSTTRA is committed to fostering a culture with the highest ethical standards to uphold our company behaviours. As part of this commitment, we will follow the S&P Global Anti-Fraud Policy to further enforce this message and provide guidance concerning any and all issues related to fraud and fraud related misconduct.

Definition of Fraud

Fraud is defined as an act of deception intended to result in a financial or personal gain. Examples of fraud include:



- Submitting false or misleading expense reports;
- Unauthorised use of company assets;
- Reporting revenue that has not been earned or does not exist;
- Submitting false or misleading financial statements;
- Misappropriation of physical assets such as a company issued laptop or intellectual property; or
- Using company funds to buy equipment or supplies for personal use or gain.

Employee responsibilities

We all have the responsibility to uphold the highest ethical standards and to conduct business in a professional manner to prevent fraudulent behaviour and activities.

If you become aware, or have suspicions, of fraudulent activities or other dishonest behaviour, you are required to report the suspected activity immediately to your manager, our HR team or our compliance team.

Confidentiality and data protection

Protecting the privacy of personal information is critical to our success. We, with the assistance of S&P Global, have a company-wide privacy compliance programme designed to protect the privacy of personal information under our control.

This is built on the core principles that we:

- Process personal information fairly and lawfully
- Collect personal information only for specified, explicit and legitimate purposes
- Process personal information only to an extent that is adequate, relevant, and not excessive
- Retain personal information only for as long as is necessary for the purpose for which it was collected
- Deploy technical and organisational safeguards to protect personal information

Personal information is defined as any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier (e.g., employee ID number, email address, home address, date of birth, etc.).

We have comprehensive policies, procedures, and systems for protecting privacy that every employee, contractor and vendor is responsible for understanding and enforcing.

We communicate our commitment to privacy and data protection to our customers, prospects, vendors, and other stakeholders through our Privacy Policy.

Vendor Risk Management also assesses and monitors vendors to ensure that they process personal information in compliance with our requirements, contractual obligations, and applicable privacy laws.

We want our customers, prospects, and other stakeholders to trust us with their personal information and know that our commitment to privacy guides how we operate.

To demonstrate our commitment to the protection of our people's privacy, our Employee Privacy Policy, which is tailored to workplace location, guides how we collect, process, transfer and store your data, and describes our general practices regarding your privacy as our employee.

For more information, please see the Employee Privacy Policy (Applicable to U.S. and India) and Employee Privacy Policy (Excluding U.S. and India).

Records and information management

It is the responsibility of all of us to help manage our information. The Records Management Policy and related standards define and guide information retention, disposition, availability, integrity, privacy, and security.

As our employee, you have any personal or property right to such records, even though you may have developed, compiled, received, or maintained them.

As the owner of the records, we are will make decisions about record storage, distribution, control, protection, retention, destruction, or use.

FCA obligations / fit and proper (SMCR)

The UK FCA regulates some of our services, and as such the FCA's Conduct Rules apply to certain people working in those businesses.

However, at OSTTRA, we believe that we should all follow the principles set by the regulator. These are known as the "Conduct Rules" and they will help set the culture and standard that we use and want to be known for.

First tier – all employees

1. You must act with integrity
2. You must act with due care, skill and diligence
3. You must be open and cooperative with regulators
4. You must pay due regard to the interests of customers and treat them fairly
5. You must observe proper standards of market conduct

The Second Tier – these apply to Senior Managers

1. You must take reasonable steps to ensure that the business of the firm for which you are responsible is controlled effectively
2. You must take reasonable steps to ensure that the business of the firm for which you are responsible complies with the relevant requirements and standards of the regulatory system

3. You must take reasonable steps to ensure that any delegation of your responsibilities is to an appropriate person and that you oversee the discharge of the delegated responsibility effectively
4. You must disclose appropriately any information of which the regulator should reasonably expect notice

Keeping the company and our employees safe

Information security

An employee must not:

- Disclose any confidential information about OSTTRA or its activities
- Disclose any confidential information about OSTTRA's customers, clients or third parties obtained while performing his or her duties
- Copy or disseminate internal communications, whether or not marked confidential, to third parties, unless authorised by the company

Some general rules:

- You should use OSTTRA's systems and property only for OSTTRA's business
- Always lock your computer when leaving your desk or you are away from your computer
- Store confidential information in a secure area. It must not be left out on desks or in areas with unrestricted access
- Apply software updates in a timely manner when prompted.
- Be aware of your surroundings especially when conducting sensitive business conversations or working on privileged, confidential, or proprietary information
- Don't use public, unprotected Wi-Fi to conduct work without a secure Virtual Private Network (VPN)
- Never send privileged, confidential or proprietary information to your personal email (this includes work related email messages or attachments)
- Never share passwords with anyone (including IT or your manager)
- Never reuse passwords from OSTTRA for external systems and websites including personal use
- Never access systems that are not reasonably related to your responsibilities
- Never view inappropriate content or repeatedly open or click on suspicious emails that exhibit "Phishing" attributes, such as unfamiliar email sources, embedded links to unknown Internet sites, requests for payments, requests for passwords and/or other confidential information
- Never store company data on non-approved cloud storage platforms (e.g., Dropbox, and public GitHub)

Right to monitor

We have implemented several policies and procedures consistent with applicable law to protect the confidentiality, integrity, and availability of our information assets. To support these efforts, we reserve the right to take possession, access, review, monitor, intercept, or conduct surveillance on any content or materials located on any OSTTRA information resource or facility.

The OSTTRA information assets you use or to which you have access are the property of OSTTRA and are provided for official business use. Our information resources should only be used for business-related purposes. Personal use of our assets should be limited to incidental use. Any communication conducted on our assets and systems is not your personal or private property, and we reserve the right to view that communication at any time. In addition, we may disclose these communications to designated OSTTRA officials, law enforcement officials or other persons when appropriate. Use of our information resources for conducting any outside business activities is strictly prohibited.

There may be times when you will access or monitor workspaces – including information stored on and usage of your company computer – for the safety of others or when otherwise deemed appropriate in the judgement of management.

All security incidents must be reported to the our Cyber Defence team as soon as possible. Security incidents include any possible or actual violations of our security practices, such as losing a piece of confidential information or leaving a laptop unlocked and unattended in public.

Reporting and enforcement

Non-retaliation

We understand that you may be apprehensive about reporting misconduct. However, you should know that we will provide support when you raise concerns in good faith, even if your concern turns out to be mistaken.

We are prohibited from threatening or retaliating in any way against people who report misconduct in good faith. Any employee, officer or director found to have engaged in threats or retaliation will be subject to disciplinary action, up to and including termination.

If you believe you have suffered any detrimental treatment as a result of reporting misconduct in good faith, please inform our head of Human Resources or Legal immediately.

What to report

You have an obligation to report any conduct or wrongdoing that violates our Code or any applicable law, rule, or regulation, regardless of whether it is about to occur or has already occurred.

You must be alert and sensitive to situations that could result in misconduct. Situations that may involve a violation of our Code or applicable laws, rules or regulations may not always be clear and may require making difficult decisions and exercising careful judgement.

Always raise concerns or questions about the propriety of a course of action or decision with a manager or a member of the compliance department.

Any concerns or questions you may have about possible wrongdoing should be raised using the procedures below.

Any concerns or questions you may have about possible wrongdoing should be raised using the procedures below.

Reporting misconduct

Whether you are raising a concern about a potential violation, or seeking advice, we have multiple resources to help guide you.

1. You can share your concern with your manager

2. Contact any member of the OSTTRA HR team who can provide further guidance
3. You can report a concern, anonymously if you choose, online or by phone to the Ethics Point Helpline. When calling the hotline, you can speak to someone who can guide you through the process
4. Contact a member of Legal or Compliance for guidance on any situation involving the Code or any other laws, policies, standards, or procedures

Good faith reporting

The effectiveness of our Code and the policies summarised in it rely on your judgement. We take concerns of misconduct very seriously and expect that any employee, officer, or director who reports misconduct does so in good faith.

Bad faith reporting or misuse of the reporting system is a violation of our Code and can be very damaging to us and your fellow colleagues.

For more information, please email info@osttra.com or contact your local OSTTRA office.

London	New York	Singapore	Stockholm	Tokyo
+44 (0) 20 7382 2200	+1 646 744 0400	+65 6372 8181	+46 8 545 25 130	+81 3 5511 6688

osttra.com