

Due Diligence Policy

Summary

The PCS Group is committed to conducting its business transparently and in accordance with the highest ethical standards. This means that The PCS Group's business must be carried out in strict compliance with all applicable laws and regulations at all times, including in the field of Bribery, Corruption, Money Laundering, Terrorist Financing and Sanctions and Trade Controls-related laws. The PCS Group has a zero-tolerance approach to any form of unethical and illegal behaviour.

This extends to The PCS Group's Business Partners, as the conduct of The PCS Group's Business Partners can have serious impacts for The PCS Group, from both a reputational and legal standpoint. Conducting appropriate, risk-based Due Diligence on Business Partners is therefore a critical part of ensuring that The PCS Group is compliant with those laws and maintains its good business reputation.

This Policy sets out certain requirements and guidance to ensure appropriate Due Diligence is carried out in respect of The PCS Group's Business Partners.

Scope

This Policy applies to all Employees in relation to any business relationships or contracts with Business Partners.

Terms and definitions

Any defined terms in this Policy are in bold. The defined terms used in this Policy shall have the following meanings.

Books and Records means accounts, books, records, invoices, correspondence, papers, and other documents that record and reflect The PCS Group's business, transactions, and other activities whether in written or in any other form (including electronic).

Bribery or Bribe means any direct or indirect offer, promise, giving, request, agreement to receive, acceptance or receipt of any payment, gift or any other advantage of value (financial or otherwise), to or from any person (including any individuals or corporate entities), in order to induce that person (or any other person) to perform their role improperly or to secure any improper benefit or advantage for The PCS Group or any other person.

Business Partner means any person who provides services to The PCS Group or who otherwise acts for and/or on behalf of The PCS Group including service providers, consultants, advisers, contractors, agents.

Compliance Officer means The PCS Group's representative who is responsible for overall compliance.

Corruption means any act done to give some improper advantage inconsistent with an official duty; the misuse of a station or office to procure some benefit either personally or for someone else contrary to an official duty.

Due Diligence Policy

Customer(s) means individual persons or companies who receive services from The PCS Group.

Director means any member of the governing Board of a corporation, association, or other incorporated body.

Due Diligence means the process undertaken to assess risk by gathering, analysing, managing, and monitoring information about an actual or potential Business Partner.

Employee means each manager, Director, employee, worker or officer hired on a permanent basis or under a fixed-term or casual employment contract by The PCS Group, including any of The PCS Group's agency workers, temporary workers, casual workers, part-time workers, trainees or interns.

Money Laundering means the process criminals use to "clean" proceeds obtained from illegal activity. Money is "laundered" by passing it through lawful businesses or activities, including routing money through various countries, whilst the nature of the illegal activity or financial transaction and the source, origin, and/or owner of the funds is hidden.

Public Official means any:

- government official or any person who is authorised by law to perform any public function;
- elected or appointed official;
- employee or officer of government and/or local authority, including, but not limited to, educational, health care and military institutions, law enforcement and customs authorities, taxation and migration services, organizations that issue state licenses, sanctions and permits;
- employee or officer of a company, enterprise, agency, business organization or entity that is wholly or partly owned or controlled by the state;
- employee or officer of international organisations
- leader and activist of a political party;
- candidate for a political office;
- members of royal families;
- honorary government officials; and
- other persons who hold a legislative, administrative, military or judicial position of any kind.

Obligations

Employee obligations

Employees are obliged to:

- read, understand and follow this Policy and any other documents aimed at its implementation;
- demonstrate ethics, integrity and accountability at all times and expect the same from other;
- direct any questions, concerns, or any known or suspected violations of this Policy to the Compliance Officer or through the channels

Due Diligence Policy

- described in the Speak Up Policy; and
- receive training as and when required by The PCS Group.

Manager obligations

In addition to the above, managers are obliged to ensure that Employees follow the requirements and instructions set out in this Policy and receive training (where required).

Compliance Officer obligations

The Compliance Officer and Compliance Facilities (including Contract Managers and Operation Managers) are:

- obliged to review and, if necessary, update this Policy and any other documents aimed at its implementation on an annual basis;
- obliged to organise training and education for relevant Employees on induction and as and when decided by The PCS Group and make sure relevant Employees complete such training and education successfully;
- responsible for the implementation of this Policy;
- obliged to raise any actual or suspected breaches of this Policy to the Board of Directors of The PCS Group as soon as is practicable; and
- obliged to provide Employees with advice and support in the matters of compliance with this Policy and relevant legislation.

Provisions

Step 1: Understanding our Business Partners and Customers

Understanding who The PCS Group's Business Partners are is key to helping The PCS Group address legal and commercial risks. The PCS Group cannot conduct business with an anonymous or fictitious company or with any Business Partner with an unclear identity or business activities.

In order to understand who our Business Partners are, and the degree of risk they present, we must conduct an appropriate level of Due Diligence before entering into any business with them. Where possible and appropriate, Employees are expected to undertake the following checks:

- Obtain key company information from the potential Business Partner or Customer. This may include:
 - company name, parent company details (if applicable), company registration number, tax number, and website URL;
 - registered office address and head office address (if applicable);
 - a copy of the certificate of incorporation (if applicable);
 - an official extract of the register of companies (or equivalent) (if applicable);
 - the articles of association of the company (if applicable);
 - names of Directors (if applicable);
 - contact details of the person who is your single point of contact;
 - the list of people authorised to sign on behalf of the company and corporate documents/powers of attorney confirming

Due Diligence Policy

- o those rights (if applicable);
- o payment address/purchase ordering address if different to head office address;
- o payment details, including the full name and address of the Business Partner's bank, as well as their account details; and
- o a confirmation on behalf of the Business Partner that all the information required above is correct and accurate.
- Know and verify the true identity of the Business Partner using reliable and independent sources, documents, data or information.
- If the Business Partner is a company, identify and verify the beneficial owners of Business Partners who have more than a 10% ownership interest in the Business Partner.
- Be familiar with the nature and history of the Business Partner's activities.

The information can be obtained from the potential Business Partner, internet searches, third party screening databases, and general market knowledge. In carrying out these checks, Employees must record the steps that they have taken, the information that they have gathered and the sources of that information. Any information that has not been obtained should be clearly identified, along with efforts to obtain such information.

All records must be kept in the relevant Books and Records.

Where an Employee is notified or becomes aware of a significant change in the information relating to the relevant Business Partner or Customer, its controlling parent or its subsidiaries (or the information previously obtained is found to have been inaccurate or incomplete), this should be reviewed and, if necessary, updated in the relevant Books and Records.

Determining whether enhanced Due Diligence is required

After the completion of the above, Employees must assess the general level of risk posed by each proposed Business Partner in order to determine whether enhanced Due Diligence is required.

The information needed to carry out this risk assessment should be based on the information obtained from the proposed Business Partner, internet searches, and general market knowledge. Employees must retain a written record in the Books and Records of the steps that are taken in assessing the risks associated with the potential Business Partner.

The risk associated with the proposed Business Partner should be assessed according to the following:

- Red flags: is there anything unusual, suspicious or otherwise different about the potential Business Partner that could give rise to Money Laundering, Terrorist Financing, Bribery and/or Corruption-related concerns?
- Services: are the services the Business Partner would be providing to their clients perceived as being a higher risk?

These are each addressed further below.

Due Diligence Policy

Red Flags

Bribery and Corruption comes in many different forms and further background information can be found in the Anti-Bribery and Corruption Policy.

Where an Employee is or becomes aware of anything unusual, suspicious or otherwise different about the Business Partner which could give rise to Bribery and/or Corruption-related concerns, this should be regarded as a red flag. Red flags include but are not limited to:

- any behaviour that would be prohibited by the Anti-Bribery and Corruption Policy;
- unusually high proposed fees for the services to be provided;
- fee arrangements, or requests for payment, that are unusual or not transparent (e.g. asking for payments to be sent to an unconnected third party, requesting payments into a foreign bank account);
- a history of Bribery or Corruption-related issues in the proposed Business Partner's organisation;
- rumours that the proposed Business Partner is or has been involved in Bribery or Corruption;
- an unclear ownership structure or lack of office or work address;
- the involvement of Public Officials in proposed Business Partner or the underlying transaction or services;
- proposals from the proposed Business Partner to make payments (not provided for by law), give gifts or provide entertainment or hospitality to Public Officials;
- where the proposed Business Partner suggests that no written agreement be put in place, or where there is otherwise a lack of visibility or clarity around the Business Partner's actual services or how it operates;
- where the proposed Business Partner is refusing to provide requested screening information or to include any Bribery and Corruption-related legal provisions in the contract.

When one or more red flags are identified in respect of a Business Partner, enhanced Due Diligence will be required.

Services

The type of services that a Business Partner provides for their own clients influences the level of risk that may be associated with such Business Partner.

Ongoing monitoring

It is not enough to make sure that there are no red flags identified with a Business Partner at the start of a new relationship. It is important that Employees remain alive to the risks associated with Business Partners and, where necessary, undertake periodic checks to ensure that the risks have not changed. The frequency and nature of the periodic checks should consider the general level of risk posed by the relationship with the Business Partner in question.

However, you must undertake a re-assessment of the relationship in any

Due Diligence Policy

circumstances where a new red flag is identified, you become aware of any information obtained in respect of the Business Partner being incorrect or incomplete, and prior to any renewal of, or change in, your relationship with the Business Partner (for example, where they will provide additional or new services).

Speaking up and reporting

Any Employee who becomes aware of breach of this Policy or any other event or circumstance that give rise to an actual or suspected breach to any Bribery, Corruption, Money Laundering, Terrorist Financing and Sanctions-related laws by any of The PCS Group's Business Partners, is obliged to escalate the issue in accordance with the Whistleblowing Policy.

Employees may report a matter anonymously (although we would encourage them to go on the record).

The PCS Group's Directors will provide comprehensive support to any of its Employees who report any issues in accordance with the Whistleblowing Policy in good faith. Retaliatory behaviour resulting from good faith reporting in accordance with the Whistleblowing Policy is never acceptable and Employees and Business Partners will not be punished for good faith reporting (even if their concern is not substantiated). Those who engage in retaliatory behaviour will be subject to disciplinary action.

Violation of this Policy

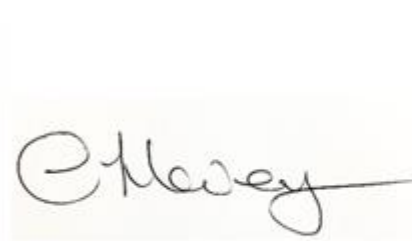
Where The PCS Group is informed of any breaches of this Policy or any event or circumstance that gives rise to an actual or suspected breach of any Bribery, Corruption, Money Laundering, Terrorist Financing, Sanctions or Trade Controls-related laws by any of The PCS Group's Business Partners, it will initiate an internal investigation thereof in accordance with the Whistleblowing Policy and involve law enforcement and other competent authorities, if necessary.

All Employees bear responsibility for the compliance with this Policy and any other documents aimed at its implementation. Failure to comply with the requirements of this Policy shall be grounds for disciplinary action up to and including dismissal.

DATES

This policy was last reviewed on 31st January 2023.

The next review will be on 1st February 2024.



Catherine Hevey
PCS Administration Director



Cert No: 11012
ISO 9001, ISO 14001,
ISO 45001

ISO 9001
ISO 14001
ISO 45001

