Tax Evasion & Anti-Money Laundering Policy

Classification	Public
Owner	Assistant Financial Controller
Approver	COO
Next Review	24 Feb 2027
Issue	v4.0
Distribution	All PQShield staff
Acknowledgement required	All PQShield staff

Introduction

Background

PQShield is committed to maintaining the highest standards of integrity and compliance with applicable laws and regulations, including those related to anti-money laundering and terrorism finance.

Applicability

This policy applies to all staff, including employees, contractors and interns working for or under the control of PQShield.

Tax Evasion

Principles

The Criminal Finances Act 2017 covers the offences of failing to prevent facilitation of UK or foreign tax evasion. It states that any relevant body which fails to prevent an associated body from criminally facilitating tax evasion will be criminally liable. Examples could include:

- Not reporting or under-reporting revenue to the tax authorities;
- Failing to report suspicions of another body committing tax evasion;
- Deliberately populating a tax return with incorrect information.

It is therefore necessary that PQShield puts in place reasonable procedures to prevent any associated persons from committing tax evasion.

Tax evasion is not the same as legal tax avoidance or planning. Tax evasion is a crime which is deliberate and dishonest. There is no minimum threshold for tax evasion - any and all tax that is deliberately not paid correctly is tax evasion.

The Policy in Operation

PQShield is committed to preventing the facilitation of tax evasion. PQShield does not permit or allow any employee or third party to engage in tax evasion.

You must not:

- Participate in any activity that may be regarded as tax evasion, or the facilitation of tax evasion, anywhere in the world;
- Enter into any arrangement with any colleague or third party that may lead to the diversion of any tax away from the relevant authorities;
- Fail to report promptly any request or demand from any colleague or third party to help them to commit a tax evasion offence, or to perform (or not perform), an action which would result in them evading tax.

You must promptly raise any concerns you may have in relation to tax evasion or the facilitation of tax evasion to the Finance Director or COO.

Anti-Money Laundering & Counter Terrorism

Principles

Money laundering is the process by which the proceeds of crime are sanitised in order to disguise their illicit origins and become legitimised. Straightforward schemes can involve large cash payments, whilst more complex schemes are likely to involve the movement of money across borders and through multiple bank accounts. Money laundering schemes typically involve three distinct stages:

- **Placement** – the process of getting criminal money into the legitimate financial system;
- **Layering** – the process of moving the money within the financial system through layers of transactions; and
- **Integration** – the process whereby the money is finally integrated into the economy, perhaps in the form of a payment for a legitimate service.

Money Laundering is a serious criminal offence that undermines the integrity of the financial system and facilitates other illegal activities including terrorism financing.

Terrorism financing refers to the illegal process of providing financial support or resources to terrorist organisations or individuals with the intention of facilitating terrorist activities.

Individuals and entities that are sanctioned are included within the framework of terrorist financing regulations.

The Policy in Operation

We acknowledge that our business operations pose a low risk of being used for money laundering activities due to the nature of our products and services. As such, the Money Laundering Regulations 2017 do not apply to the PQShield. However, we recognise the importance of implementing this Tax Evasion & Anti-Money Laundering Policy.

If a colleague knows or suspects that another colleague, customer, or supplier is involved in money laundering activities, they are required to report such suspicions to the Senior Compliance Manager. The Senior Compliance Manager will then take appropriate action in accordance with the company's policies and procedures, and any applicable laws.

Furthermore, as part of our Export & Trade Compliance Policy, we screen prospective customers for sanctions before onboarding them, and we strictly will not deal with any sanctioned entities or people.

This policy will be reviewed periodically to ensure its effectiveness and compliance with evolving laws and regulations. Updates will be made as necessary to address any changes in the company's operations or regulatory requirements.

Compliance & Monitoring

- Compliance with this and all other policies and procedures is mandatory;
- Any breach of policy may result in disciplinary action, up to and including dismissal.

Monitoring

Compliance with the processes and guidance contained within this policy will be highlighted through notification of any Information Security and other Governance breaches whereby an investigation will identify non-compliance and then seek to understand and address the reasons for non-compliance.

Audit & Review

Internal Review

Compliance with this policy will be monitored through Information Security Internal Audits, and by other management checks as required.

External Review

Inspections by external auditors may be carried out from time to time.

As part of these activities, external inspectors may ask to view internal records. Supervised access to such records must be provided where requested.

Copies of records must not be retained by an inspector unless this has been specifically approved by the CEO or COO.

Policy Review

This policy will be reviewed by the CEO or their nominated delegate at regular intervals, not exceeding one year, or when business changes warrant it as part of the continual service improvement process.