TRUST. WELL EARNED.	BRUSH Group Anti-Money Laundering Policy	**Document Number**	BRUSH-LE/BPL/0003
		Issue	C

Department	Legal	**Approver**	D Jordan	**Signature**		**Date**	07/11/2022

THIS PAGE IS INTENTIONALLY BLANK

TRUST. WELL EARNED.

BRUSH Group
Anti-Money Laundering Policy

The BRUSH Anti-Money Laundering Policy must be followed by anyone who works for or represents BRUSH, including directors, officers, employees, agents, distributors, and business associates working for or on behalf of any BRUSH entity, including, but not limited to:

BRUSH Group Ltd., BRUSH Transformers Ltd., Hawker Siddeley Switchgear Ltd., Aprenda Ltd., and Hawker Siddeley Switchgear Pty Ltd.

Employees must gain an understanding of the Anti-Money Laundering Policy, and ensure that its principles are fully applied in relevant areas of their job role

Policy statement and objectives

BRUSH Group (**"Group"**) is committed to preventing money laundering. The Group and its employees can commit offences by dealing in the proceeds of any person's crime, and the Group takes seriously the responsibility of ensuring its business is not used for the purposes of money laundering and are committed to best practice in this area. The Group requires all employees of the Group and its business units to adhere to this policy in order to prevent the use of the Group and its products and services being used for the purposes of money laundering. Adherence to the policy is critical to ensure that all business units in the Group, regardless of geographical location, comply with its obligations in respect of preventing money laundering. This policy complements the Anti-Bribery and Corruption, Trade Compliance, Whistleblowing and Document Retention Policies.

What is money laundering?

Money laundering is the process by which the proceeds of crime are converted into assets which appear to have a legitimate origin, so that they can be retained permanently, or recycled to fund further crime. The "proceeds of crime" are, broadly speaking, money or other property which results from any criminal conduct, including (for example) bribery and corruption, tax evasion, modern slavery, and breaches of competition law.

- Placement - Placement is the process of placing criminal property into the financial system. It might be done by breaking up large sums of cash into smaller amounts or by using a series of financial instruments (such as cheques or money orders) deposited at different locations.
- Layering - Layering is the process of moving money that has been placed in the financial system in order to obscure its criminal origin. It is usually achieved through multiple complex transactions often involving complicated offshore company structures and trusts.
- Integration - Once the origin of the money is disguised it ultimately must reappear in the financial system as legitimate funds. This process involves investing the money in legitimate businesses and other investments such as property purchases or setting up trusts.

Given the nature of BRUSH's activities, a key money laundering risk for the Group is "trade-based money laundering". This is the use of trade transactions to disguise the origins of criminal proceeds, for example by over- or under-invoicing goods and services, or over- and under-shipments of goods and services.

Customer and supplier due diligence

As part of the Group's commitment to prevent money laundering, Group employees must ensure that they complete adequate counterparty due diligence on all customers, suppliers, and other counterparties to reduce the risk of the Group dealing in the proceeds of crime or being used by a counterparty who wishes to launder money.

The counterparty due diligence process that must be followed is:

- Ascertain and verify the counterparties identity
- The counterparty's identity should be verified based on documents, data or information obtained from a reliable and independent source, e.g. checking with the organisation's website to confirm the business address, checking the governmental registry of companies in the country in which the counterparty is based;
    - Ascertainment of Ultimate Beneficial Owner (UBO). The beneficial owner(s) of the counterparty should be identified. The UBO is the natural person who either ultimately controls the counterparty, or directly or indirectly owns more than 25% of the counterpart.
    - Consider whether there is any other person on whose behalf or for whose benefit a transaction or activity is being conducted, if not the counterparty, and if so, identify their beneficial owner(s).

- Establish the purpose of the business relationship. If the counterparty is a new one, the rationale for wanting to transact with us should be established.
- Ask the counterparty to explain the reason for the transaction in question and, in this context, pay attention to the "red flags" set out below.

Potential Sanctions Issues

- If a counterparty is located in a jurisdiction subject to sanctions, additional due diligence must be completed in accordance with the Trading sanctions policy. Bear in mind that individuals, companies, and specific assets (e.g., aircraft, ships), can be subject to sanctions. If there are any concerns these may apply, report such concerns to the BRUSH Group General Counsel.

Reporting requirements/red flags

The following circumstances should be seen as "red flags" in relation to the risk of the Group dealing in the proceeds of crime or being used for the purposes of money laundering. Report any of the below, or any wider concerns in relation to a transaction/contract, to the BRUSH General Counsel for purposes of determining whether enhanced due diligence and/or making appropriate confidential notification(s) to the relevant authority / authorities is warranted.

- A counterparty provides minimal, vague, or fictitious information about itself or the reasons for wanting to do business.
- A counterparty is overly secret or evasive about its ultimate beneficial owner.
- The counterparty's proposed business activity is inconsistent with its wider business profile.
- A counterparty provides false or counterfeited documentation.
- A counterparty is using an agent or intermediary without good reason.
- A counterparty is actively avoiding personal contact without good reason.
- A counterparty wishes to pay or receive payment in cash. Cash receipts from counterparties and cash payments should be actively discouraged. No payment to the Group will be accepted in cash if it exceeds £1,000. Cash payments made by the Group are only authorised where they amount to less than £1000. An exception to this may be made in specified circumstances in relation to cash advances to employees. In such cases the Group Policy on cash advances to employees must be followed.
- A counterparty is based in a country where there is a higher risk of criminality or money laundering, such as a High-Risk Country under the Trading Sanctions Policy.
- The counterparty is the subject of allegations of criminal conduct.
- The counterparty requests payments to or from a third party, or country other than the country where it is incorporated or where the transaction is based.
- A counterparty makes an overpayment requiring a refund.
- There are significant discrepancies between a counterparty's invoices, shipments, and contract with the Group.
- When raising concerns, Group employees should be mindful about making any communications that could prejudice investigations by law enforcement authorities, contrary to applicable law.

Money laundering enforcement is on the increase in Europe and is a focus of law enforcement authorities in the UK. A key risk for companies outside the regulated sector is "trade-based money laundering". This factsheet outlines some key trends and developments in this risk area.

AML enforcement and penalties are increasing.

According to public sources , there were 58 AML penalties in 2019 totalling US$8.14 billion, compared to 29 penalties totalling US$4.27 billion in 2018. Although historically the US has been the most active enforcer, enforcement in Europe is increasing in 2019, European AML penalties totalled US$5.8 billion, exceeding US

penalties of US$2.2 billion. In the UK, the National Crime Agency (NCA) estimates that hundreds of billions of pounds may be laundered through the UK annually . In recent years, the UK has strengthened the powers of law enforcement agencies to deal with money laundering. For example, in 2018 Unexplained Wealth Orders were introduced, which require a person to explain how they obtained certain property. In addition, where corporates are investigated for criminality, the authorities may include money laundering charges: for example, in May 2017 the UK Serious Fraud Office announced that it is investigating Petrofac PLC suspected bribery, corruption and money laundering.

Although there is a particular focus on money laundering in the regulated sector, non-regulated companies can also commit money laundering offences if they deal in the proceeds of crime. For example, if a company obtains a contract through bribery, the proceeds of the contract will constitute the proceeds of crime. Similarly, any benefit that a company may obtain through other forms of corporate criminality, such as modern slavery or anti-competitive conduct, will constitute the proceeds of crime. A company which then deals in the proceeds of crime, for example by receiving the proceeds of a corrupt contract, may commit laundering offences – even if the company is not seeking to "launder" those proceeds in the sense typically understood.

Where a company suspects that it may have engaged in conduct that could have given rise to proceeds of crime, it should carefully consider whether a report ought to be made to the authorities. In the UK for example, it is possible to seek consent from the NCA in order to deal with the proceeds of crime. The company should also bear in mind that its auditors may have independent obligations to report suspected money laundering to the authorities, as in the UK.

Trade-based money laundering" is a particular risk to trading companies.

"Trade-based money laundering" (TBML) is the use of trade transactions to disguise the origins of criminal proceeds. For example, a supplier could over-invoice goods or describe them as higher quality (and therefore higher value) than they really are, so that the customer effectively transfers additional value to the supplier in the form of an excess payment. A recent report from the US General Accountability Office indicates that, in the US at least, TBML may be increasing partly because of US financial institutions' improved compliance with AML regulations . In the UK, the NCA believes that there are specialist "International Controller Networks" that launder money for criminals through various methods, including TBML .

However, TBML is difficult to identify because it is integrated into the economy through trade transactions. It is therefore important for companies to include TBML as a type of risk to in their compliance risk assessments and, in the course of business, to be alert to "red flags" that may point to potential TBML. The NCA has provided the following informational graphic setting out example "red flags" of TBML: