GOBRISK TECHNOLOGIES PRIVATE LIMITED

Merchant Onboarding Policy

Version 9
17 March 2025

PROPOSED BY	Guneshwor Singh Laitonjam, Head of Compliance and MLRO
APPROVED & ACCEPTED BY	Sanjay Tripathy, Director Nilesh Pathak, Director Indunath Chaudhary, Director

The document draws and consolidates the guidance and processes from various policies that have been adopted by the company since inception and revised from time to time.

Table of Contents

1. Introduction

GoBrisk Technologies Private Limited (hereinafter referred to as 'BRISKPE' or 'the Company') incorporated on February 21, 2023, is a Mumbai-based financial services technology startup.

As per RBI/2023-24/80 CO.DPSS.POLC.No.S-786/02-14-008/2023-24 dated October 31, 2023,Payment Aggregator- Cross Border (PAs-CB) are entities that facilitate cross-border payment transactions for import and export of permissible goods and services in online mode.

The Guidelines on Regulation of Payment Aggregators and Payment Gateways ('PA Guidelines') dated March 17, 2020, issued by the RBI prescribes a PA to put in place a Merchant Onboarding Policy. In accordance with the said PA Guidelines and PA-CB Regulations, BRISKPE has formulated this Merchant Onboarding Policy (the 'Policy') duly approved by the Board of Directors (the 'Board') outlining the onboarding process BRISKPE will follow to conduct thorough due diligence of Merchants who will be availing the services of BRISKPE.

2. Objective

The PA Guidelines in conjunction with PA-CB Regulations underscore the necessity of thorough scrutiny in assessing the appropriateness of the Merchants that are integrated into the system. This is to ensure that these Merchants harbor no ill intentions of deceiving customers or engaging in the sale of fraudulent, counterfeit, or banned goods.

Considering these stipulations, BRISKPE has established a systematic procedure to conduct comprehensive background checks and previous record verification of the Merchants. This is to ascertain that only fitting Merchants are integrated, thereby safeguarding BRISKPE from any potential reputational or monetary hazards while offering its services.

This policy shall be read in conjunction with other BRISKPE Policies such as KYC AML CFT Policy, Sanctions and Screening Policy, Transaction Monitoring Policy and ABC Policy at a minimum.

3. Definitions

a) ***"Customer"*** – end-user who has purchased goods or availed services from the Merchant and has made payment for them using BRISKPE's PA - Cross Border services.

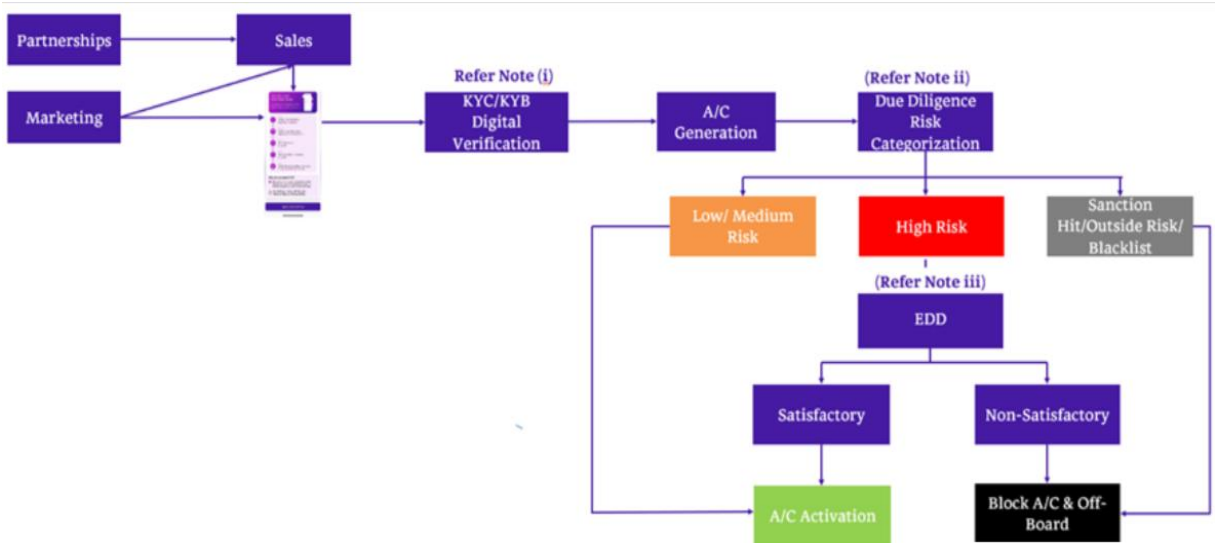
b) ***"Merchants"*** – an individual or legal entity (ies) with whom the Company has entered into a contract (Merchant Agreement) for the purpose of providing payment solutions/ services.

c) ***"Suspicious transaction"*** – a transaction including an attempted transaction, whether or not made in cash, which, to a person acting in good faith:

i. gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence in the Schedule to the Prevention of Money Laundering Act (PMLA), regardless of the value involved; or
ii. appears to be made in circumstances of unusual or unjustified complexity; or
iii. appears to not have economic rationale or bona-fide purpose; or
iv. gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

Transaction involving financing of the activities relating to terrorism includes transaction involving funds suspected to be linked or related to, or to be used for terrorism, terrorist acts or by a terrorist, terrorist organization or those who finance or are attempting to finance terrorism.

4. Merchant Onboarding and KYC Process



4.1 Complete Know Your Customer (KYC) & Know Your Business (KYB):

The Merchant is onboarded through a digital process which requires validation of ID/Address and Business Documents as outlined in Section 3.4 of the **KYC AML CFT Policy** whether in assisted manner by sales, partner or virtually. This step also categorizes the Merchants into various risk categories.

4.2 Merchant Due Diligence (MDD):

This step is completed in combination of online and offline process before Merchant onboarding is completed or flagged for Enhanced Due Diligence (EDD) as per risk triggers.

4.3 Enhanced Due Diligence:

Enhance Due Diligence (EDD) refers to performing a higher level of CDD in higher risk situations such as Merchants or products defined as potentially high-risk. EDD may be applied because of

a. Customer being classified as high risk in accordance with the Company's methodology.
b. Customers that are in High-Risk Countries outlined by FATF Black and Grey Listing, or RBI circulars from time to time
c. Industries as outlined in Appendix 2 of the KYC AML CFT Policy
d. Confirm Sanctions and screening results,
e. Suspicious transaction reporting outcome,
f. Outcome of Law Enforcement enquiry

Scrutinizing a customer's transactions more closely and more frequently for consistency with the Company's knowledge of that Customer etc. and this may result in the Customer not being allowed to transact on the platform; more intensified monitoring; product/service limitation, exited if already onboarded etc. as deemed appropriate. Additional provisions have been built in the Sanctions and Screening Policy and Transaction Monitoring policy that triggers completion of EDD for the customer.

4.4 Risk Categorization:

Merchants are categorized in three risk categories named as "Low Risk", "Medium Risk" and "High Risk." post determining the risk score as per parameters defined in KYC AML CFT policy.

4.5 Reliance on Third Parties

The Company may partner in future with certain service providers in its business and operational processes. However, for the purpose of complying with any of its AML/CFT obligations, the Company does not rely on any third parties to complete screening on our behalf.

- The Company will confirm that the decision-making tasks related to compliance with KYC norms are not delegated to an external entity.
- Furthermore, at the initiation of an account-based relationship, the Company can depend on the CDD performed by a third party, subject to the following conditions:
    i. The Company obtains records or information about the customer due diligence conducted by the third party immediately from the third party or from the Central KYC Records Registry.

ii. The Company will take the necessary measures to ensure that copies of identification data and other relevant documents related to the customer's due diligence requirements are available from the third party promptly upon request.
iii. The third party is regulated, supervised, or monitored for compliance with customer due diligence and record-keeping requirements in accordance with the requirements and obligations under the PML Act.
iv. The third party does not operate from a country or jurisdiction that is assessed as High Risk.

- The Company will bear the ultimate responsibility for CDD and implement Enhanced Due Diligence measures, as applicable.

5. KYC Process

5.1 KYC Process for Indian Merchants

- **ID Verification:**

The person registering on BRISKPE's portal needs to identify him/herself with their Permanent Account Number (PAN), issued by Income Tax Department of India. BRISKPE validates the PAN through APIs.
The process has been enhanced with liveliness check and validation of user's live image from the image of ID.

- **Address Validation:**

The person registering on the portal needs to validate him/herself with their Aadhaar Number, issued by UIDAI. BRISKPE validates the Aadhaar details i.e. Address, Name matching with PAN through OTP authentication method. The process is completed with Consent based APIs.
In the event the Merchant isn't providing consent, the onboarding is to be completed in an offline manner with necessary approvals from Compliance, and Business Head.

- **Business PAN:**

Legal entity's name and active ID is verified using their Permanent Account Number (PAN), issued by Income Tax Department of India. BRISKPE validates the PAN through APIs. This step also validates the availability of Active GSTIN mapped to this PAN.

- **Business GSTIN**

Business GSTIN is fetched using the linked PAN and address of the Merchant is also fetched using GSTIN details. This step also highlights the entity type, based on which subsequent flow capturing Director details from MCA/UBO details shall be identified.
For non-GST registered firms, separate approval is required from the Business Head for manual onboarding at this step.

- **Business Website:**

Active Business Website is mandatory for Auto Approval.

- **Business Segment:**

The customer selects the business segments which are acceptable. *For customer segments such as "Other" an EDD is flagged by the system.*

- **UBO and Director Details:**

This step is different for types of entities like Private Limited/ Public Limited/ LLP, Partnership Firms and Proprietorship and ensures identification of active business, Directors/ Partners/ UBOs.

- **Bank Account:**

The Bank account number and IFSC code are to be entered by the applicant and BRISKPE does beneficiary validation and fetches the business name and address of the Bank Branch. The entity name matching with bank records and business PAN is a mandatory requirement for onboarding.

These details are used for settlement of the funds to Merchants post collection of export receivables from overseas buyers.

In the absence of any valid information as mentioned above (except the website) the onboarding shall go on hold and approval would be required from the business head and operations head after completing manual risk checks to permit onboarding.

5.2 KYC Process for Overseas Merchants

- **ID & Address Validation:**

Depending on the type of the legal entity, BRISKPE will collect the following identification documents from the Merchant:

In case of Non-Resident Indians (NRIs) and Persons of Indian Origin (PIOs), as defined in Foreign Exchange Management (Deposit) Regulations, 2016 {FEMA 5(R)},or a Non-Indian Nationals looking forward to initiating or continuing Overseas Seller relationship and/or happens to act in any or all capacity as Directors, UBO, Authorized Representative, the names of the relevant persons holding senior management position; officers or employees holding an attorney to transact on the company's behalf for Overseas/Domestic Seller relationship ; an original certified copy of their valid Passport (at least 6 months before expiry) ; or any equivalent e-documents showing the Nationality of the Individual capturing clear Full Name and address which is certified by any one of the following, may be obtained to complete the CDD process:

- authorised officials of overseas branches of Scheduled Commercial Banks registered in India,
- branches of overseas banks with whom Indian banks have relationships,
- Notary Public abroad,

- Court Magistrate,
- Judge,
- Indian Embassy/Consulate General in the country where the non-resident customer resides.

The documents provided by foreign Merchant may be in English or may be accompanied by a copy of translation in English (where document is not available in English). Further, the documents and its translation need to be certified by the Merchant or its authorized person.

- **Business registration document:**

  The identification of the legal entity is verified using constitution documents such as Certification of Incorporation, Certification of Business, Registration Certificate, or Memorandum and Articles of Association, Partnership Deeds etc. as prevalent in the jurisdiction of the Merchant. Documents required for each Merchant type are being duly elaborated on Section 3.4 of our KYC AML CFT Policy. The CDD procedure shall be as per RBI KYC MD .

- **Business Website:**

  Active Business Website is mandatory for Auto Approval.

- **Business Segment:**

  Merchant may select the business segments which are acceptable by BRISKPE and provide registration documents, as applicable.

- **UBO and Director Details:**

  Ultimate Beneficial owner is duly identified as per the entity type and CDD is duly performed all UBO's meeting the 10% threshold requirements.

- **Bank Statement:**
  The latest bank account statement in the Merchant's name along with cancelled cheque is collected from the Merchant. The entity name matching with bank records is a mandatory requirement for onboarding.

Note: The above documents provided by Overseas Merchant should be in English or should be accompanied by a copy of translation in English (where document is not available in English). Further, the documents and their translation need to be certified by the Merchant or its authorized person.

In addition to the above, BRISKPE will also ensure the following while onboarding Foreign Merchants:

- BRISKPE will consider the country risk attributable to the domicile of the Foreign Merchant and India's foreign trade policies and trade sanctions at the time of on boarding.

- BRISKPE will collect and validate documents, subject to local laws and regulations of the country of domicile the Foreign Merchant, or in accordance with the instructions issued by the RBI from time to time.

- In case the per unit price of goods/services offered by a Foreign Merchant is more than INR 2,50,000 (Indian Rupees two lakh fifty thousand), BRISKPE will ensure contractually and operationally that the Foreign Merchant obtains at the time of check out, the permanent account number (PAN) number of the end customer. As part of buyer due diligence, BRISKPE will:

    - Obtain the full name, OTP verified mobile number and the Officially Valid Documents (OVD)/ Permanent Account Number (PAN) of the Indian Buyer.
    - Validate the OVD/ PAN details using APIs; and
    - Match the details received from OVD/ PAN issuing entity with the details provided by the Indian Buyer
    - nature of business and purpose of purchase.

  Transaction is processed further if due diligence is successful, else it is terminated.

- BRISKPE will restrict the Foreign Merchants availing the PA-CB-I product from selling goods/services that have a per unit price exceeding INR 25,00,000 (Indian Rupees twenty-five lakhs). As part of its onboarding check and periodic review, it will ensure that the merchant confirms that none of its good/services has a per unit price exceeding INR 25,00,000 (Indian Rupees twenty-five lakhs). As an additional measure, BRISKPE will consider imposing transaction limits to ensure compliance and mitigate any AML/ fraud related risk.

6. Merchant Due Diligence

The Company will proceed with a comprehensive background verification process on receipt of the KYC documents from the Merchant as per the CDD requirement based on client type as defined in KYC AML CFT Policy. This verification aims to authenticate the Merchant's intentions, business model, and purpose.

- Conducting necessary assessments to ensure that the Merchant does not pose as potential fraudsters or shell companies, and do not engage in the sale of fake, prohibited, or counterfeit products.

- Reviewing the Merchant's web presence, including affiliated press articles, domain name, social media pages, and online customer ratings, to establish a comprehensive profile and assess reputation.

- Verifying if the Merchant's website clearly outlines offered products/services, About Us, , Contact Us, Product Checkout),

- Scrutinizing the business, track record, and verifying commercial history.

- Screening Merchant names against watchlist databases such as the UN Sanctions List, OFAC SDN List, RBI Unlawful Activities (Prevention) Act, 1967, WMD, FIU-IND list and other similar lists released periodically. *This section is to be read in conjunction with the Sanctions* policy for detail screening lists.

- Additionally, Merchants will undergo screening against Politically Exposed Persons (PEPs) lists and Negative databases. A video or in-person meeting is mandatory with the AR/UBO residing in India. V-CIP shall not be conducted for individuals outside of India geolocation.

If a Merchant fails to meet the above requirements, the Company will request clarification or additional details as necessary. Failure to provide satisfactory clarification or details will result in the Merchant's application being declined.

The above verification will enable the Company to categorise the Merchants into low, medium and high-risk categories, thereby enabling the Company to appropriately conduct Due Diligence and Enhanced Due Diligence as applicable.

Note: This section is to be read in conjunction with the Company's KYC AML CFT Policy.

7. Enhanced Due Diligence (EDD)

Merchants who have been flagged for EDD at the time of onboarding are screened by Operations using the below EDD procedure. An EDD is performed for all the cases which are referred to during onboarding either at the time of Digital On-boarding or during MDD.

- EDD shall require determining their Source of Wealth (SOW) and/or Source of Fund (SOF) either by using a detailed Ministry of Corporate Affairs (MCA) reports or GST Returns, Bank Statements, Audited Financials to validate business revenues for domestic/cross-border trade or business activities.

- In the event of a newly incorporated company, the decision is to be taken based on Directors/Partners/Proprietor conduct, behaviors, social presence, previous associations, bank statements etc.

- Method of Merchant acquisition to be understood and mode of Goods/service delivery to be verified.

- Proof of Goods/Service delivery & Invoice to be verified.

- Categories of Merchants for High-Risk/Medium-Risk/Low-Risk while recommending the case for approval to Compliance Officer/Operations Head.

Once EDD is completed, the recommendation is to be submitted to the Compliance Officer and Business Head for further action w.r.t. approval or rejection.

Any Merchant going through the EDD process and approved is to be closely monitored for the first three months and upon any red flag, the client should be marked for de-boarding without allowing any new transactions.

8. Ongoing Monitoring

BRISKPE follows a differentiated approach to monitor transactions of Merchants falling in different risk categories.

The transactions of Merchants assessed to be of “Low risk” and “Medium risk” are subject to standard monitoring measures and the transactions of Merchants assessed to be of “High risk” are subject to enhanced monitoring measures.

Merchants with a “low risk” rating are those where BRISKPE determines that the country risk, product/service/transaction risk and delivery channel risk are not high. BRISKPE defines appropriate thresholds such as country list, product/industry list, product/service type, amount thresholds and other appropriate parameters for risk categorization as covered above in MDD and Risk categorization Process Note. Merchants in any of the risk categories are name-screened against Sanctions lists, PEPs and Adverse media checks and are subject to transaction monitoring.

For ongoing monitoring, the Company has put in place processes commensurate with the size and complexity of the business to:

- Monitor the transactions done by the Customers on its platform to ensure that those are in line with the normal Business Relations with Customers; and
- Detect, investigate and report suspicious, complex, unusually large or unusual patterns of transactions undertaken throughout the course of Business Relations.

9. Transaction Monitoring Process:

BRISKPE obtains from the Merchants the transaction level data points such as description of product/service, quantity, unit price, involved parties and shipment details (including carrier details wherever available) as well as underlying commercial documents (such as invoice, agreement) and transport documents where applicable (such as bill of lading/airway bill of lading).

All relevant data points collected, their transactions booked on the platform and associated documentation obtained from the Merchants are logged in a central repository.

The Operation Team reviews the data daily. Any red flags/ escalations are made to the Compliance team for further review, investigation and reporting as appropriate. BRISKPE pays special attention to all complex, unusually large or unusual patterns of transactions, undertaken throughout the course of business relations, that have no apparent or visible economic or lawful purpose.

Upon identification of any high-risk parameter, enhanced Merchant due diligence is triggered. For all cases categorized as high-risk, such Merchants will be subject to EDD and ongoing monitoring for each transaction will be conducted.

In cases where a transaction raises doubts or suspicions, BRISKPE's employee will request additional information or clarification as may be required to resolve such doubts or suspicions. In all cases when a clarification process is undertaken, the transactions are reported to the Compliance team and Senior Management. Further, in cases where the clarification does not resolve the doubts or suspicious circumstances, BRISKPE shall file a SAR/STR about the transaction with the FIU-IND as appropriate

Where there are any reasonable grounds for suspicion that existing Business Relations with a Customer relate to money laundering or terrorism financing (but not enough evidence), and where the Company considers it appropriate to retain the Merchant:

- the Company will substantiate and document the reasons for retaining the Merchant; and
- the Merchant's Business Relations with the Company will be subject to commensurate risk mitigation measures, including enhanced ongoing monitoring, which will include obtaining the approval from the respective Business Head (designee) and MLRO (designee) with a detailed rationale.

If the Company has identified a suspicious transaction or other cause for concern and has filed 3 or more repetitive STR in relation to the relevant Merchant, the Company may consider terminating Business Relations with that Merchant.

The Company may also consider terminating Business Relations with a Merchant if the conduct of Enhanced Due Diligence or request for additional clarification has revealed a more than reasonable suspicion of ML/TF, or if the Merchant's ML/TF risk profile exceeds the Company's capacity to mitigate it.

BRISKPE will terminate business relations with a Merchant immediately were

- the Merchant is known to be or reasonably suspected of being a sanctioned individual/entity; or
- the Merchant is blacklisted or linked to one or more blacklisted accounts with BRISKPE.

Below mentioned are some of the monitoring parameters examples for Merchants:

- ✓ **Buyer-seller collusion/ghost transaction:**
  - A buyer and a seller pair doing several large transactions in quick succession.
  - Several buyers with similar email ID (first+last+digit@domain.com) are buying from the same seller.

- ✓ **Velocity Patterns:**
  - The same buyer is making several purchases from a single seller in quick succession.
  - The same buyer is making purchases for different sellers.

- ✓ **Inconsistent Transactions:**
  - Transactions where there is inconsistency in the names of the parties declared in the transaction, KYB documents, underlying transaction documents (e.g. invoice, bill of lading) and the names in the bank accounts of the buyer and seller.

Note: This section is to be read in conjunction with the Typology Section of the Company's Transaction Monitoring Policy.

10. Merchant Risk

Given the risks associated with the PA-CB Business, Merchant risk monitoring program plays a vital role in managing Merchant risks during a Merchant's lifecycle with BRISKPE. Digital payments aggregation processing and facilitation of cross-border payment generates significant risk due to the contingent liability inherent in the digital payment processing relationship that BRISKPE has with Merchants, who in turn provide goods/services to the customers.

Once the background verification of a Merchant is successfully completed, BRISKPE assigns a value score between a 0 to 5 against each parameter of (with 0 denoting highest risk and 5 the lowest risk) and assigns a risk score to the Merchant based parameters defined in Merchant risk policy. The extent of monitoring of the Merchant and its transactions is aligned with the risk category of the Merchant which means a high-risk Merchant will be subjected to more intensified monitoring.

Below mentioned are the frequencies of review required for a Merchant as per the risk levels:

Risk Level	**Frequency of review**
Low	Every Ten years
Medium	Every Eight years
High	Every Two years

11. Merchant Off-Boarding

BRISKPE envisages that a Merchant could be deactivated either through voluntary exit request from the Merchant or terminated by BRISKPE.

11.1. Deactivation due to request by Merchant:

Deactivation due to voluntary exit request by Merchant refers to voluntary exit from their relationship with BRISKPE. The reasons could include business restructuring, changes in strategy or simply deciding to cease operations. It's common in business practice in business and the specifics would depend on the circumstances of each Merchant.

11.2 Merchant de-activation by BRISKPE:

BRISKPE will undertake ongoing monitoring and due diligence of all its Merchants and the transactions conducted by them. Thus, in case BRISKPE finds that the Merchant is in violation, then BRISKPE will seek clarification regarding the same from the Merchant. In case BRISKPE is not satisfied with the Merchant's clarification, it will initiate termination proceedings against the Merchant.

A list of common reasons that will dictate the circumstances under which a Merchant account may be terminated are as under:

- Violation of Terms of Service.
- High Risk.
- Excessive Chargebacks.
- Non-Compliance.
- Suspicious Activity.
- Failure to provide documentation.
- Lack of Payment.
- Change in Business Model; and
- Reputation Risk.

11.3 Merchant Deactivation Process:

The deactivation request in case of voluntary exit by Merchant involves the simple steps stated as under*:

- Check Terms: Review Terms and Conditions
- Settle Balances: Clear Outstanding Balances
- Contact Provider: Reach out to BRISKPE through emails or customer service.
- Provide Info: Give necessary details
- Follow steps: Follow BRISKPE's instructions
- Confirm Closure: Confirm deactivation
- Documents: Keep records for reference

**BRISKPE follows a similar process in case of Merchant termination by BRISKPE.*

12. Changes/ Updation to Merchant Information

The Company is committed to maintaining the accuracy of Merchant information in its systems.

For any modifications or updates to the Merchant's information, the Merchant is required to submit a request to the Company via their registered mobile number or email id, accompanied by relevant documents. The Onboarding team will then authenticate these details prior to updating them in the system.

13. Review of Policy

BRISKPE will review the Policy annually or earlier, if required, considering any material changes in regulatory framework or for business or operational reasons. Any subsequent changes will form part of the Policy after the approval of the Board.

14. Version History

Versions	Author	Date of Review	Board Approval	Approved By	Change History
1*	*Sanjay Tripathy, Nilesh Pathak, Indunath Chaudhary,*	*01.05.2023*			
2*	*Sanjay Tripathy, Nilesh Pathak, Indunath Chaudhary,*	*15.06.2023*			
3*	*Sanjay Tripathy, Nilesh Pathak, Indunath Chaudhary,*	*10.07.2023*			
4*	*Sanjay Tripathy, Nilesh Pathak, Indunath Chaudhary,*	*28.07.2023*			
5*	*Sanjay Tripathy, Nilesh Pathak, Indunath Chaudhary,*	*01.11.2023*			
6	*Sanjay Tripathy, Nilesh Pathak, Indunath Chaudhary,*	*09.07.2024*			
7	*Sanjay Tripathy, Nilesh Pathak, Indunath Chaudhary,*	*30.09.2024*	30.09.2024	Board	Created
8	Guneshwor Singh Laitonjam	18.12.2024	18.12.2024	Board	**Updated various sections related to:** Appendix 7 – Risk Scoring
9	Guneshwor Singh Laitonjam	17 March 2025	17 March 2025	Board	Updated: Objective added to read in conjunction with other relevant BRISKPE policies Sec 4.5 Reliance on Third Parties

					5.2 KYC Process for Overseas Individuals and Merchants update. 10. Review frequency changed to match RBI KYC MD Removed all appendixes as these can be referred from KYC/AML/CFT policy to avoid duplication.

**The versions from 1 to 4 were known as KYC_KYB Policy*