BR/VX AML and Financial Crime Policy

Last updated on [January 18, 2026]

This AML, Sanctions and Financial Crime Policy Summary ("Policy Summary") describes the principles applied by BR/VX in seeking to prevent the use of the BR/VX Digital Interface for money laundering, terrorist financing, sanctions evasion, fraud, market abuse and other prohibited or unlawful activity.

BR/VX Digital Interface does not permit use of the Interface for unlawful activity. BR/VX may apply risk-based technical, compliance and access-control measures to protect the integrity of the Interface, its users, its infrastructure providers and the broader market.

This Policy Summary should be read together with the BR/VX Terms of Use, Privacy Policy and any other applicable policies published through the BR/VX Digital Interface.

1. Purpose and Scope

BR/VX seeks to maintain a secure and responsible environment for users of the BR/VX Digital Interface.

This Policy Summary applies to users who access, connect to, interact with or otherwise use the Interface, including through connected wallets, APIs, community features, referral features, partner features or other supported functionality.

The purpose of this Policy Summary is to explain that BR/VX may take reasonable and proportionate measures to:

- identify and mitigate potential financial crime risk;
- restrict access from prohibited jurisdictions;
- screen public blockchain addresses and transaction-related information;
- identify sanctions exposure;
- detect suspicious, fraudulent or abusive activity;
- prevent market manipulation and prohibited trading conduct;
- investigate potential misuse of the Interface;
- comply with applicable legal obligations;
- protect users, infrastructure providers and the integrity of the Interface.

2. Non-Custodial and Interface-First Position

BR/VX provides access to decentralized and non-custodial interface features.

BR/VX does not:

- custody user assets;
- hold user private keys;
- control non-custodial wallets;
- independently initiate transfers from user wallets;
- centrally control public blockchain networks;
- control or reverse public blockchain transactions once submitted to a blockchain.

However, BR/VX may restrict, suspend or terminate access to the BR/VX Digital Interface where required by law, sanctions obligations, security requirements, internal risk controls, third-party infrastructure requirements or this Policy Summary.

The fact that a blockchain transaction may be public, decentralized or technically irreversible does not prevent BR/VX from taking steps to restrict access to the Interface or associated features.

3. Prohibited Activity

Users must not access or use the BR/VX Digital Interface for, in connection with, or to facilitate:

- money laundering;
- terrorist financing;
- proliferation financing;
- sanctions evasion;
- fraud;
- theft or misuse of stolen digital assets;
- ransomware-related activity;
- phishing;
- malware distribution;
- hacking or unauthorized access;
- extortion;
- trafficking in illicit goods or services;
- exploitation or abuse of vulnerable persons;
- corruption or bribery;
- market manipulation;
- wash trading;
- spoofing;
- layering;
- front-running;
- insider trading;
- deceptive or misleading trading practices;
- referral fraud;
- bonus or incentive abuse;

- use of false identity, location or eligibility information;
- attempts to circumvent geoblocking, screening, sanctions controls or access restrictions;
- any conduct that violates applicable law, regulation, sanction, court order or regulatory requirement.

Users must not use VPNs, proxies, remote access tools, false location information, nominee arrangements, false identity information or other means to circumvent geographical, sanctions, eligibility or compliance restrictions.

4. Restricted Persons

A “Restricted Person” includes any individual, entity, wallet, organization or other person that:

- is subject to sanctions, asset freezes, trade restrictions or other restrictive measures imposed or administered by the United Nations, the United States, the European Union, the United Kingdom or any other applicable authority;
- appears on, is owned or controlled by, or acts on behalf of a person appearing on an applicable sanctions or restricted-party list;
- is located in, ordinarily resident in, incorporated in, organized in, has a registered office in, or is operating from a Restricted Jurisdiction;
- uses the Interface on behalf of a Restricted Person;
- is involved in activity reasonably suspected to be unlawful, fraudulent, abusive or inconsistent with this Policy Summary;
- has attempted to bypass or evade access controls, sanctions screening, jurisdictional restrictions or other compliance measures.

For the purposes of this Policy Summary, ownership or control may include direct or indirect ownership, control, influence or benefit, including through intermediaries, nominee arrangements, affiliates or related parties.

5. Restricted Jurisdictions

The BR/VX Digital Interface is not available to users who reside in, are located in, are incorporated or organized in, have a registered office or principal place of business in, or otherwise access the Interface from a Restricted Jurisdiction.

For initial operational purposes, Restricted Jurisdictions include:

- United States of America;
- Canada;
- United Kingdom;
- People’s Republic of China;
- Democratic People’s Republic of Korea;
- Russian Federation;

- Cuba;
- Iran;
- Venezuela;
- any comprehensively sanctioned jurisdiction, territory or region;
- Crimea;
- the so-called Donetsk People's Republic region;
- the so-called Luhansk People's Republic region;
- any jurisdiction, territory or region subject to comprehensive country-wide, regional or equivalent economic sanctions;
- any jurisdiction determined by BR/VX to present unacceptable legal, sanctions, regulatory, financial crime, technical or operational risk.

BR/VX may also restrict access from additional jurisdictions based on local law, licensing requirements, regulatory risk, third-party provider requirements, sanctions developments or internal risk assessment.

The list of Restricted Jurisdictions may be amended at any time without prior notice. Users are responsible for reviewing the current Restricted Jurisdictions Notice before accessing or using the Interface.

6. Public Blockchain Address Screening

BR/VX may use risk-based blockchain analytics, sanctions screening, fraud prevention and security tools to assess public blockchain addresses, transactions, smart contract interactions and related on-chain activity.

This may include screening for exposure to or association with:

- sanctioned addresses;
- terrorist financing;
- ransomware;
- malware;
- phishing;
- stolen funds;
- hacks or exploits;
- dark market activity;
- fraud;
- scams;
- mixer or obfuscation-related activity;
- high-risk service providers;
- market abuse indicators;
- other illicit or prohibited activity.

BR/VX may use information obtained from public blockchains, blockchain analytics providers, sanctions screening providers, infrastructure providers, law enforcement notices, public sources or other reliable sources for these purposes.

The use of screening tools does not constitute a representation that any wallet, transaction or user has been definitively identified as unlawful. Screening outcomes may be used as part of a broader risk-based assessment.

7. Risk-Based Compliance Measures

BR/VX may apply different levels of review, restriction or monitoring depending on the nature, severity and context of a potential risk.

Measures may include:

- access restrictions;
- geoblocking;
- IP or location-based controls;
- wallet screening;
- transaction monitoring;
- enhanced review of unusual activity;
- requests for additional information;
- identity or eligibility verification, where necessary;
- source-of-funds or source-of-wealth review, where necessary;
- suspension of specific features;
- restriction of referral, partner or incentive programs;
- removal of community access;
- API restrictions;
- account or profile limitations, where applicable;
- reporting to competent authorities where required or appropriate;
- termination of access to the Interface.

BR/VX may take such measures before, during or after a user's interaction with the Interface.

8. Information Requests and Verification

BR/VX may request information, confirmations, documentation or verification where reasonably necessary to:

- comply with applicable law;
- assess sanctions or restricted-jurisdiction exposure;
- investigate suspected fraud or abuse;
- assess suspicious wallet or transaction activity;
- evaluate partner, affiliate or incentive eligibility;

- protect the security of the Interface;
- respond to lawful requests from regulators, courts or law enforcement;
- resolve disputes, complaints or security incidents.

A user's refusal or failure to provide requested information may result in restriction, suspension or termination of access to some or all features of the BR/VX Digital Interface.

9. Suspicious Activity and Market Integrity

BR/VX may monitor the use of the Digital Interface for signs of suspicious, abusive or potentially unlawful activity.

This may include review of conduct that appears to involve:

- unusual transaction patterns;
- repeated failed or reversed transactions;
- manipulation or attempted manipulation;
- wash trading;
- coordinated or deceptive trading activity;
- fraudulent referral behavior;
- false or misleading representations;
- circumvention of access restrictions;
- abnormal API activity;
- automated activity designed to impair, overload or exploit the Interface;
- activity associated with suspicious or high-risk blockchain addresses;
- activity inconsistent with the stated purpose or expected use of the Interface.

BR/VX may investigate such activity and take appropriate action consistent with this Policy Summary, the Terms of Use and applicable law.

10. Cooperation With Authorities and Service Providers

BR/VX may cooperate with competent regulators, law enforcement agencies, courts, sanctions authorities, blockchain analytics providers, security vendors, infrastructure providers, professional advisers and other parties where required or permitted by applicable law.

BR/VX may disclose relevant information where necessary to:

- comply with legal obligations;
- respond to a lawful request;
- protect users or third parties;
- prevent fraud, financial crime or market abuse;
- enforce the Terms of Use;
- defend legal claims;

- protect the security, integrity or operation of the BR/VX Digital Interface.

Any processing or disclosure of personal data will be subject to the BR/VX Privacy Policy and applicable law.

11. User Representations

By accessing or using the BR/VX Digital Interface, each user represents and warrants that:

- they are not a Restricted Person;
- they are not accessing the Interface from a Restricted Jurisdiction;
- they are not acting on behalf of a Restricted Person;
- they will not use the Interface to violate applicable law;
- they will not use the Interface to evade sanctions, geoblocking or compliance controls;
- their wallet, assets and transactions are not connected to unlawful activity;
- they will provide accurate information if BR/VX requests it;
- they will promptly update BR/VX if their location, residency, eligibility or ownership/control status changes;
- they understand that BR/VX may restrict or terminate access where required for legal, sanctions, security or risk-management reasons.

12. No Assurance of Continued Access

Access to the BR/VX Digital Interface may be restricted, suspended or terminated at any time where BR/VX determines that continued access may create legal, sanctions, regulatory, financial crime, security, operational or reputational risk.

BR/VX does not guarantee that any user, wallet, jurisdiction, asset, feature, API, referral program, community feature or trading-related functionality will remain available.

Any decision to restrict access may be taken without prior notice where necessary to comply with law, preserve security, prevent misuse or protect the integrity of the Interface.

13. Updates to This Policy Summary

BR/VX may revise this Policy Summary from time to time to reflect legal, regulatory, sanctions, operational, technical or risk-management developments.

The updated version will be published through the BR/VX Digital Interface or other appropriate communication channels.

The “Last updated” date at the top of this Policy Summary indicates the latest version.

Continued use of the BR/VX Digital Interface after an updated Policy Summary becomes effective constitutes acknowledgement of the updated Policy Summary.

14. Contact

For questions regarding this Policy Summary, suspected financial crime, sanctions concerns, abuse reports or compliance matters, contact:

Support: [support@brvx.com]