Global Sanctions Policy

Document Version Control

Version:	5.2
Date of Issue:	25 July 2025

Document Approval and Sign-Off

Version No:	Department / Approval Forum:	Approval Date:
5.2	Todd Mcelduff, Global Head of Enterprise Compliance	24 July 2025
	Noah Perlman, Global Chief Compliance Officer	25 July 2025

Retired Document

Name of Document	Date Issued
Global Sanctions Policy (v.5.1)	27 May 2025
Global Sanctions Policy (v.5.0)	06 March 2025
Global Sanctions Policy (v4.0)	09 August 2024
Global Sanctions Policy (v3.5)	22 February 2024
Global Sanctions Policy (v3.4)	24 October 2023
Global Sanctions Policy (v3.3)	06 March 2023
Global Sanctions Policy (v3.2)	04 January 2023
Global Sanctions Policy (v3.1)	15 November 2022
Global Sanctions Policy (v3.0)	11 March 2022
Sanctions Manual (v2.0)	5 November 2020
Sanctions Manual (v1.0)	12 March 2020

Table of Contents

1.0 Purpose & Scope

Sanctions are a policy tool that sanctions authorities including national governments and multinational organisations use to constrain and deter perceived security threats, to prevent or suppress criminal activity, or to encourage a change in, or to apply pressure to, a target country or regime. While national and multinational sanctions regimes vary in their content, rules, and restrictions, they generally fall into the following three programme categories:

1. Comprehensive Sanctions (the countries or territories comprehensively targeted by these programmes are defined as “Sensitive Sanctioned Country” or “SSC”)
2. Selective Sanctions (activity-based)
3. List-Based Sanctions (targeting individuals, entities, vessels, and aircraft whose names appear on sanctions lists and, in many cases, entities, vessels, and aircraft owned or controlled by the foregoing individuals or entities)

Binance is committed to complying with applicable sanctions legislation in the jurisdictions it is registered, licensed, or operates. The Binance Global Sanctions Policy (the “BGSP” or “Policy”) establishes the minimum operating requirements and standards to mitigate potential compliance, regulatory and reputational risks associated with potential violations and evasions of sanctions legislation and the risk of conducting any business with sanctioned parties.

This Policy applies sanctions laws, regulations and regulatory guidelines under the regulatory regimes imposed by the United Nations (“UN”) and the United States (“US”) to Binance’s operations globally. EU legislative requirements apply to Binance’s activities in EU Member States (including Binance entities that are registered or licensed in EU Member States), unless otherwise noted. Other Binance entities may be subject to sanctions regulations in their local jurisdictions. Binance must comply with local laws and sanctions obligations in the jurisdiction where it is registered, licensed, or operates in the event of any conflict between this Policy and local laws and regulations applicable to specific Binance entities, and must apply the higher of the standard of this Policy or the local standard where applicable.

Many jurisdictions also have Counter Terrorist Financing (“CTF”) legislation, which forms part of the Binance Global Anti-Money Laundering Program. However, the BGSP administers the applicable legislation relating to individuals, entities and organizations designated as terrorists, which generally has similar asset freezing and regulatory reporting requirements as List-Based Sanctions.

1.1 Application

The BGSP applies to Binance.com and wholly and majority owned legal entities of Binance. The BGSP also applies to Binance’s subsidiaries, affiliates,[1] offices, directors, officers, employees, consultants, contingents, contractors, casual workers, agency workers, and interns in all fiat and crypto currencies in which it may transact.

This Policy applies to customers as well as non-customers such as vendors, suppliers, service providers, or any person or entity acting on behalf of Binance. Non-customers also include external counterparty and fiat channel partners, and other non-affiliate agents for the Binance Group. For non-customers, the vendor management policy and processes, as well as the respective contractual agreements, should include the relevant standards and controls to ensure Binance does not establish or continue business relationships with Designated Persons or with parties that pose material sanctions risk.

Employees who fail to comply with this Policy may be subject to disciplinary action, up to and including

[1] Affiliates could include minority-owned investments of Binance, as identified by the Global Head of Sanctions on a case-by-case basis.

termination.

The Global Sanctions Recusal Statement (in Appendix III) supports this Policy's objective to mitigate the risk of a Binance employee undertaking an activity that may breach sanctions applicable to them by virtue of their nationality, residency or location.

1.2 Key Policy Outcomes

The BGSP is established to ensure the Binance Group conducts business in accordance with applicable sanctions laws, regulations and restrictions in the jurisdictions where it is registered, licensed or operates and to communicate Binance's Sanctions Risk Appetite through terms and conditions acknowledged by customers and other relevant parties.

This Policy is intended to:

- ensure strong governance and risk management throughout Binance to properly manage and mitigate sanctions risks;
- promote active and full cooperation with regulatory and law enforcement authorities with investigations, prosecutions and forfeiture actions relating to sanctions;
- provide overall guidance to the Binance Group on the minimum sanctions compliance operating standards and on specific local requirements contained in Country Addenda for the purposes of compliance with applicable sanctions laws, regulations and restrictions (including local sanctions laws and regulations);
- advise Binance employees of their obligations under this Policy and promote Binance employees' awareness to detect, escalate and/or report any sanctions issues (including Designated Persons or any activity involving individuals, entities or organisations suspected of sanctions evasion activities, material sanctions risk or potential sanctions breaches).

1.3 Approval & Annual Review

This Policy must be reviewed and approved, at least annually, by the Binance Board of Directors.

Sanctions laws, regulations and restrictions are generally subject to changes with immediate effect. Accordingly, the Global Chief Compliance Officer ("GCCO") is authorized to approve interim amendments to this Policy. Supplementary Global Sanctions Communications ("GSCs") will be issued to the Binance Group outlining the impact of the amendments along with any required actions to support compliance with latest amendments. Additionally, material changes to applicable sanctions regulations that are not immediately incorporated into the BGSP will be communicated through GSCs.

1.4 Three Lines of Defence - Key Sanctions Related Roles & Responsibilities

Binance uses a Three Lines of Defence model in respect of Financial Crime Compliance (including Sanctions Compliance).

- **First Line of Defence ("1LOD") - Owns & Manages Risks**

  Global Lines of Business, Global Operations, and other business unit process owners are considered the 1LOD, responsible for identifying risks (in close alignment with the Enterprise Compliance) relating to Sanctions Compliance and for implementing and maintaining adequate procedures and controls to mitigate these risks.

  Front Office and user facing employees in particular have the responsibility to remain vigilant in detecting and escalating customer activity potentially involving or relating to sanctions risk and sanctions evasion to Global Sanctions.

- **Second Line of Defence ("2LOD") - Oversees Risks & Risk Controls**

  Global Compliance acts as the 2LOD risk stewards with Global Sanctions having responsibility for establishing and maintaining the BGSP and sets guidelines for managing operations risks to address legal and regulatory requirements in relation to sanctions risk and BGSP requirements. It has an advisory role to the 1LOD, and performs assessment on the adequacy and effectiveness of the controls proposed and implemented by the 1LOD.

- **Third Line of Defence ("3LOD") - Provides Independent Risk Assurance**

  Under the direction of the Audit and Finance Committee, Internal Audit is the 3LOD responsible for providing independent assurance of both the 1LOD and 2LOD to ensure the Binance Group has implemented a robust Financial Crime Compliance Program, including Sanctions, and assessing the adequacy and effectiveness of internal controls.

  The Group may engage with qualified external third parties to independently evaluate the Financial Crime Compliance Program and controls for purposes of reporting to the Senior Management or to related committees delegated by the Senior Management.

Appendix II sets out the key sanctions related roles and responsibilities.

1.5 Dispensations & Country Addendum

All Binance entities must comply with the BGSP. Where a Binance entity is unable to comply with a specific requirement of this Policy due to operational/system constraints or local legislative requirements that conflict with or impose a higher standard than the BGSP requirements, it must request a dispensation from Global Sanctions. The submission should include a clear rationale for the dispensation and identify the appropriate local country management approval, control owners, and relevant stakeholders who were consulted.

In the event of any conflict between the standards articulated in the BGSP and local regulations, the local business should ensure they are in full compliance with local legal requirements. In the event that local legislative requirements impose a higher standard than the BGSP requirements or vice versa, the local business should ensure they are in full compliance with the higher standard.

Sanctions related dispensations must be approved by the Global Head of Sanctions ("GHS") and will only be considered if adequate mitigating controls could be put in place or are in place to reduce the level of risk to an appropriate level. Dispensations are granted for a maximum of 12 months and must be

documented in the relevant Country Addendum. Approved Country Addenda form part of the BGSP and should be read in the context of, and in conjunction with the BGSP. All defined terms in the Addenda have the same meaning as defined in the BGSP, unless otherwise indicated. The Country Addenda apply to Binance Group entities operating in a number of countries (the latest list of which is located at Sanctions Compliance Framework), and to their employees.

1.6 Policy Breaches

A breach of the Policy is defined as non-compliance with a requirement of the BGSP, such as a relationship established/transaction processed that is not supported by an approved policy dispensation or Transaction Sanctions Exception (see details in Appendix I). Whenever there is a potential breach of this Policy, it should be immediately reported to Global Sanctions (via SanctionsAdvisoryBot) and the Country MLRO, where necessary.

Global Sanctions and the Country MLRO (where necessary), in consultation with Legal, must determine whether a policy breach could also be a potential breach of sanctions laws or regulations. Where a breach of the Policy could be a potential breach of sanctions laws or regulations, the MLRO in the country impacted must ensure required reports are made to the relevant sanctions authorities without delay. In consultation with Global Sanctions, the MLRO must also consider the root cause of the breach and ensure a corrective action plan is completed promptly, where necessary.

1.7 Effective Date

This Policy is effective 25 July 2025.

2.0 Minimum Control Requirements

The Binance Group does not undertake transactions

- with customers that are Designated Persons on a Global Sanctions List (refer to the Global Sanctions Operating Framework (“GSOF”) - Appendix I(A)) or, where applicable, Local Sanctions List (refer to the GSOF - Appendix I(B)),
- with individuals or entities ordinarily resident, established, or located in an SSC, or
- that are prohibited in the jurisdictions where it is registered, licensed, or operates.

2.1 Customer Due Diligence & Risk Assessment

Customer Due Diligence (“CDD”) is a crucial control to mitigate sanctions risk among the Binance customer population by obtaining an appropriate level of Know Your Customer ("KYC”) or Know Your Business (“KYB”) information and understanding customer activity and product usage as defined by the Global Anti-Money Laundering and Countering Terrorism Financing Policy (“Global AML Policy”).

The Binance Group ensures that where there are indicators of potential sanctions risk noted from CDD, Investigations, Transactions Monitoring, or the like, Enhanced Due Diligence (“EDD”), Sanctions Exposure Questionnaire (“SEQ”), or SSC Nationals Sanctions Questionnaire (“SSCQ”) must be completed to identify and document whether a potential new customer or an existing customer has material direct or indirect sanctions risk exposure as set out in Appendix I. Indicators of potential sanctions risk include but not limited to:

- entity customers with a high risk nature of business and/or SSC nationals or residents as related

parties (including UBOs, controllers and directors)[2];
- individual customers whose place of birth are within SSCs;
- customers having significant dealings with or involving SSCs or jurisdictions that are considered high sanctions risks; or
- customers whose source of wealth or source of funds are from SSCs or from jurisdictions that are considered high sanctions risks.

Where there is a potentially material sanctions risk perceived from, or the involvement of a Designated Person in, a prospective or existing customer relationship, it should be escalated to Global Sanctions for guidance.

2.1.1 Periodic & Event Triggered Customer Reviews

All Business Lines, with the assistance of Compliance Operations, must conduct (i) periodic customer reviews following a risk-based approach in accordance with the time frames defined by the Global AML Policy in respect of customers assessed as having potentially high sanctions risks; and/or (ii) ad hoc customer reviews immediately following a sanctions related trigger event, which is any event that suggests the customer's sanctions risk has changed, such as:

- the customer's IP address / web timezone suggesting they might be resident in an SSC, their source of funds or wealth is from an SSC, their country of nationality is that of an SSC, or they may have dealings with or involving SSCs
- the customer, including related parties of an entity customer are added to any of the sanctions lists used for screening
- payments to or from the customer are blocked or rejected for sanctions reasons
- information received suggesting the customer attempted to circumvent sanctions or Binance sanctions related controls

Such reviews (including having the customer complete an EDD, SEQ or SSCQ, if applicable) should assess and document any new or increased sanctions risk in relation to the customer and ensure that the sanctions risk exposure remains within Binance's risk appetite.

2.2 Sanctions Representations and Warranties

If appropriate, Global Sanctions may recommend additional sanctions representation and/or warranty be provided by a customer who is identified as posing elevated sanctions risk during onboarding or at any time during the customer relationship.

2.3 Customer and Non-Customer Sanctions Screening

Binance has established name screening procedures (as part of Binance KYC controls) to comply with regulatory obligations, mitigate risk, and identify customers and non-customers such as vendors who are included on regulatory sanctions and CTF lists. Binance maintains and implements two categories of sanctions screening lists - Global Sanctions Lists and Local Sanctions Lists - and engages third-party service providers to provide regulatory lists for the Global Sanctions Lists and Local Sanctions Lists for sanctions and CTF screening. The Global Screening Steering Committee is responsible for oversight of the systems used in screening, including system configuration and lists used in screening.

Global Sanctions Lists are required to be screened by Binance against its entire customer base and transactions (where applicable) to detect potential sanctions and terrorist financing nexus. The Global Sanctions Lists include the regulatory lists issued by the UN and jurisdictions identified in Appendix I(A) of the GSOF. In addition, local MLROs are required to identify any local sanctions list that are required under

[2] Refer to KYB Program V.4.0

local sanctions and CTF legislation to be screened against customers of the local registered or licensed entity. These are referred to as Local Sanctions Lists and are identified in Appendix I(B) of the GSOF. The fact that a Binance entity screens against a Global Sanctions List or Local Sanctions List does not necessarily mean that the laws or regulations of the jurisdiction that issues each list are legally applicable to the Binance entity conducting the screening. Please refer to Appendix I of the GSOF for the details of Global Sanctions Lists and Local Sanctions Lists.

Customer sanctions screening must be conducted when opening a new account for an existing customer or establishing a new customer relationship, on an ongoing basis throughout the customer relationship in response to changes in customer information (e.g., change of user information) or updates to the foregoing sanctions screening lists. Sanctions screening must be completed prior to onboarding new customers and no transaction is permitted prior to completion of such screening.

Non-customer/third-party sanctions screening must be conducted in a similar way as customer sanctions screening to mitigate the potential sanctions risk of Binance transacting with Designated Persons. For third party screening, including suppliers, distributors, contractors, or any other entity that a company might partner with, please refer to Third Party Due Diligence for details.

2.4 Transaction Monitoring

The Binance Group must implement and maintain procedures and controls to conduct automated real-time on-chain screening of transaction details and other available identifying information (e.g., originator, beneficiary, originating and beneficiary exchanges, VC addresses and underlying transactional data) to identify and prevent transactions associated with Designated Persons, persons on internal watchlists, or persons in SSCs.

Post-transaction on-chain and off-chain monitoring should also be conducted to identify transactions involving virtual currency (“VC”) addresses or other identifying information believed to be associated with Designated Persons, SSCs, prohibited domains, or potential sanctions evasion.

2.5 Geolocation Controls

Geofencing creates a virtual perimeter around a real-world location, such as a country or region, using location data from a user's Internet Protocol (“IP”) address or device to enable (or disable) specific actions when the user enters or exits the geofenced location.

While IP addresses are useful to identify a customer’s physical location, they may not be reliable as IP addresses are the most accessible location data points and vulnerable to manipulation and are imprecise. There are various inexpensive and easy-to-use tools available that can mask a user’s location including Virtual Private Networks (“VPNs”) and Domain Name System (“DNS”) proxies.

It is critical that Binance maintains controls to detect and restrict activity originating from an IP address geolocated to an SSC or a jurisdiction that is subject to customer relationship or transaction restrictions in certain jurisdictions such as the EU (e.g., Russia and Belarus). In particular, Binance should implement controls to detect where a customer’s location, as indicated by their IP address, is believed to be false and their actual location or place of residence is in an SSC or restricted jurisdiction.

The Binance Group must implement effective geolocation controls to:

1. restrict customer access and/or reject transactions from IP addresses geolocated to SSCs or other jurisdictions subject to sanctions restrictions;

2. exit relationships where customers repeatedly attempt to access Binance services from an SSC or restricted jurisdiction; and

3. detect customers for further review and restrict (as appropriate) who may be attempting to access services through the use of VPNs or other IP spoofing software/techniques.

2.6 Travel Rule

Certain jurisdictions have adopted regulations to implement FATF Recommendation 16 (the "Travel Rule"). Such regulations require virtual asset service providers to collect, verify, transmit and hold personal identifiable information (PII) of originators and beneficiaries of cryptocurrency transfers. This includes, among other information, the name and address of originators and beneficiaries. Some Travel Rule regulations may also require real-time transaction screening against sanctions lists published by the UNSC and/or local sanctions lists.

All transactions, including on-chain and off-chain cryptocurrency transfers, are subject to the Transaction Restrictions described in Appendix I Section E. This means that Binance must implement sanctions screening controls to identify transfers involving Designated Persons or SSCs when sufficient originator and beneficiary information is made available as a result of Travel Rule regulations. This includes screening against any applicable Local Sanctions Lists as required under local regulation.

2.7 Account Restrictions and Blocking/Freezing of Assets

The Binance Group must ensure that all customer accounts and/or other property associated with the following persons are restricted and/or blocked/frozen:

- Designated Persons on a Global Sanctions List or, where applicable, on a Local Sanctions List
- Individuals or entities ordinarily resident, established, or located in an SSC
- Detected as having accessed the account from an SSC IP address temporarily

All Binance entities must apply appropriate restrictions and/or controls to these restricted accounts and to ensure no transactions are processed or products and services provided.

In the event it is prohibited under local law to restrict an account or block/freeze property, this must be immediately escalated to Global Sanctions by the local MLRO.

Approval is required from Global Sanctions before the return, release or transfer of any cryptocurrency or other property in an account that has been restricted for sanctions risk reasons.

The Business Line and Compliance Operations must ensure adequate procedures are implemented to lift restrictions on an account or unblock/unfreeze property when it is determined that sanctions no longer apply to an account.

Where a customer relies upon a license granted by a relevant sanctions authority to engage in transactions otherwise prohibited by applicable sanctions legislation, Binance shall require the customer to produce a copy of the license for review by Global Sanctions and Legal. Please refer to Appendix I E(ii) for details on Transaction Sanctions Exceptions.

2.8 Customer Offboarding Management

Where the Binance Group decides to terminate a customer relationship due to sanctions risk, customer offboarding should be handled in accordance with the Global Compliance Account Restrictions (Freeze Actions) SOP, Account Restrictions - Freeze/WOM Actions Checklist, and Offboarding Procedures .

A customer relationship is only considered as fully offboarded once all accounts, products, open positions and services have been fully closed, cancelled or transferred outside any Binance platform. Where a customer relationship is in the process of being offboarded for sanctions reasons and cryptocurrency or

other property continues to be held by Binance, the account must be restricted to withdrawal only and if there is a potential sanctions hit against the account, no further withdrawal is permitted until it is reviewed by Global Sanctions. Records of customers offboarded for sanctions reasons must be retained by Global Sanctions.

2.9 Mergers & Acquisitions, Joint Ventures and Other New Investments

Sanctions due diligence must be conducted when Binance makes new investments, including mergers & acquisitions, joint ventures, and partnerships, in order to assess potential sanctions risks entailed in the new investments and/or associated with the new targets and/or partners. Within 90 days upon closing of a new investment, the new entity/new business associated with the new investment is required to adopt the BGSP requirements and formulate a work plan for implementing sanctions controls with specified milestones.

3.0 Global Anti-Financial Crime Enterprise-Wide Risk Assessment

Binance is required to assess its AML, CTF, sanctions, and other financial crime risk exposure across the entire business. This Anti-Financial Crime Enterprise-Wide Risk Assessment ("AFC EWRA") process is an essential part of developing and implementing Binance's approach to financial crime prevention and combating terrorist financing.

Binance's global AFC EWRA exercise consists of:

- Business Risk Assessments (BRA)
- Product Family Risk Assessments (P(F)RA)
- Aggregation of the P(F)RA and BRA into the EWRA.

AFC EWRA focuses on three areas – inherent risk, control, and residual risk. Inherent risk assessment refers to the evaluation/quantification of the overall risk profile based on the business operations, strategy, activity, and model. In terms of control assessment, it includes the assessment of the effectiveness of key financial crime internal controls, taking into consideration factors such as anti-financial crime resources, training, record keeping, MI, policies and procedures, KYC/KYB, suspicious activity patterns and trends, AML monitoring and reporting, sanctions screening, reporting as well as governance. Residual risk assessment refers to the assessment of the remainder risk after the successful implementation of controls that effectively mitigate the assessed inherent risk and taking into account other mitigating factors.

For details on AFC EWRA, please refer to the Global Anti Financial Crime Enterprise Wide Risk Assessment Scoring Methodology (Version 2.0), and the Global Anti Financial Crime Enterprise Wide Risk Assessment (AFC EWRA) 2024.

4.0 Regulatory Reporting & External Queries

Binance must immediately freeze any property, including crypto assets and any fiat currency (and the rights to these assets), of customers identified as Designated Persons on any of the Global Sanctions Lists or, where applicable, Local Sanctions Lists. Sanctions and CTF laws may require a Binance entity to report information relating to assets held for Designated Persons. Such reporting must be made in the format and within the time frames defined in applicable legislation.

All sanctions and terrorist property related reporting and communications, including administrative demands for information to relevant sanctions authorities or regulatory or law enforcement agencies must be responded to by Investigations and/or MLROs in coordination with Global Sanctions and Legal within time frames set by the relevant sanctions authority or regulatory or law enforcement agency, while

ensuring responses to these requests are consistent with local laws and regulations.

All Binance entities must cooperate fully with all sanctions related inquiries and requests from sanctions authorities, government, local regulatory and law enforcement agencies pertaining to investigations, prosecutions, and forfeiture actions. Binance entities must designate liaison staff, to ensure local processes and procedures are in place, to respond promptly to any lawful information requests, while ensuring responses to these requests are consistent with local laws and regulations (in particular local data privacy laws and regulations).

The Binance Group may, on the advice of the GHS and Legal, make a voluntary self-disclosure to the relevant sanctions authority of non-compliance with any applicable sanctions regulation.

5.0 Sanctions Evasion

No Binance employee shall, in any way, assist or facilitate a customer to evade or circumvent applicable sanctions and CTF regulations, the BGSP, or Binance sanctions related controls.

The facilitation prohibition also restricts the type of advice or other guidance a Binance employee may provide to anyone regarding activities related to Designated Persons under this Policy, including advice on how to structure a transaction to avoid specific sanctions prohibitions or Binance controls. Examples include:

- Any suggestion that sanctions laws or regulations or BGSP don't need to be followed
- Customers' refusal to follow Binance Terms of Use that includes sanctions compliance obligations for customers
- Asking leading questions that guide customers to provide answers that conceal potential sanctions risk
- Guidance to customers on how to submit instructions and what details to provide or omit to conceal potential sanctions risk
- A customer attempts to withhold, alter or misstate a name or re-submits a transaction rejected by Binance, but strips out information or provides revised details (for e.g. new/revised name of the counterparty or counterparty's address), that appears to be made in an effort to evade applicable sanctions laws or Binance screening controls

Binance employees must promptly escalate any evasion attempt by anyone to Global Sanctions via SanctionsAdvisoryBot or to InternalAuditBot (a whistleblowing channel).

6.0 Training

Training is one of the fundamental pillars of Binance's Financial Crime Risk Management Framework and contributes to promoting a strong compliance culture.

(i) Annual Sanctions Training

All Binance employees must complete annual *Global Sanctions Mandatory Training,* which is embedded into the Financial Crime Compliance Training. All new and existing employees must complete this training within 30 days of onboarding/assignment unless otherwise noted. Sanctions training content must be reviewed at least annually and refreshed (where necessary) with the approval of GHS.

(ii) High Risk Role Training

Binance employees who perform roles considered to be high risk for sanctions must receive additional targeted training relevant to their role to supplement the *Global Sanctions Mandatory Training*. The training is delivered annually, virtually, or in person where practical, by Global Sanctions.

Sanctions High Risk Roles include roles that entail customer contact, process customer transactions, or otherwise evaluate customer data. Training records are maintained by Global Compliance Learning to ensure completion.

High Risk Role Training must be reviewed at least annually and refreshed (where necessary) with the approval of GHS.

7.0 Record Keeping

All records relating to sanctions and CTF matters must be maintained in accordance with regulations in each jurisdiction Binance is registered, licensed, or operates and for a minimum of 5 years unless otherwise noted.

DEFINITIONS & FREQUENTLY USED TERMS

Term	Description
BGSP	Binance Global Sanctions Policy
Blocked/Frozen Account	A Binance account that holds assets of a customer whose account is restricted or whose property is blocked/frozen due to sanctions risk or an applicable sanctions requirement..
BO	Beneficial Owner (as defined in the Global AML Policy)
CDD	Customer Due Diligence
Country Addendum	Where it is required to comply with local sanctions laws and regulations additional to, more stringent than, or different than this Policy, a local Binance entity is required to use the Approved Template (located in https://confluence.toolsfdg.net/display/CMPL/Sanctions+Compliance+Framework) to document these local sanctions laws and regulations in the respective Country Addendum to the BGSP and to obtain approval from GHC and GSSC accordingly.
CTF	Counter Terrorist Financing
Designated Person	This refers to individuals or entities that are identified under a regulatory sanctions or CTF list. For the purposes of the BGSP, a Designated Person also includes an entity being owned or controlled by a Designated Person such that sanctions would apply according to the standards defined in the applicable regulation.
Direct Exposure	Refer to Appendix I section E.
EEA	European Economic Area
EDD	Enhanced Due Diligence (refer to the Global AML Policy for details)
EU	European Union
EU Person	A National of a Member State, of a country member of the EEA or of Switzerland, or a natural person having a temporary or permanent residence permit in the EU, EEA or Switzerland.
GCCO	Global Chief Compliance Officer
GHS	Global Head of Sanctions
Global Sanctions	Team supporting the GHS, setting Group-wide policy and supporting the business as well as advising Binance executives on sanctions related matters.
Global Sanctions Lists	Set out in Appendix I(A) of the GSOF. These are the lists that Binance uses for sanctions and CTF screening globally.
GMLRO	Global Money Laundering Reporting Officer
GSOF	Global Sanctions Operating Framework
Indirect Risk Exposure	Sanctions risk that arises from a customer's exposure to a Designated Person or SSC outside of the customer's relationship with Binance.
Local Sanctions Lists	Set out in Appendix I(B) of the GSOF. These are the lists that the local Binance entity uses for sanctions and CTF screening pursuant to local regulatory requirements.
License	An authorization issued by a sanctions authority that allows certain categories of transactions to take place that would otherwise be prohibited by a sanctions program. Types of licenses include “general” licenses, which are issued for use by the public, and “specific” licenses, which are issued for the benefit of specific persons named in the license.

Term	Description
MLRO	Money Laundering Reporting Officer or In-Country Head of Compliance is used interchangeably. MLROs have responsibility at the local level for AML, Sanctions and AB&C compliance.
National	An individual who has the nationality of a country based on birth, residency status, naturalisation, or other standards defined under national law. Some individuals may be nationals of multiple countries.
OFAC	Office of Foreign Assets Control, administering US Sanctions Programs.
Restricted Accounts	Accounts that are temporarily or permanently inhibited due to a potential or confirmed sanctions risk. The property in the account may also be blocked/frozen.
Risk Appetite	Risk appetite refers to the level of risk that Binance is prepared to accept in relation to a customer, transaction, or business activity before action is deemed necessary to reduce or eliminate exposure to the acceptable risk. Binance maintains a defined risk appetite for activities related to sanctions as set out in Appendix I.
Russian / Belarusian National	Any natural person who holds the citizenship of the Russian Federation or the Republic of Belarus (wherever that person may be located /domiciled).
SDN	Specially Designated National. Persons who are identified on OFAC's List of Specially Designated Nationals and Blocked Persons. Legal entities owned 50% or more by SDNs are also subject to OFAC sanctions.
SSC	Sensitive Sanctioned Countries, currently including Cuba, North Korea, Iran, and the regions of Crimea, the so-called Donetsk People's Republic and the so-called Luhansk People's Republic
UBO	Ultimate Beneficial Owner, i.e., the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.
VA	Virtual Asset, a digital representation of an item that has value in a specific environment, including crypto, virtual currency and NFTs
VC	Virtual Currency

Appendix I: Sanctions Programmes

This Appendix sets out Binance's Sanctions Risk Appetite and restrictions and prohibitions on customer relationships and transactions relating to:

- Sensitive Sanctioned Countries (SSCs)
- Selective Sanctions (activity-based)
- List-Based Sanctions (targeting individuals, entities, vessels, and aircraft whose names appear on sanctions lists and, in many cases, entities, vessels, and aircraft owned or controlled by the foregoing individuals or entities)

A. Comprehensive Sanctions and SSCs

Comprehensive Sanctions seek to prohibit most financial and commercial interaction with a specific territory or country. Generally (with few exceptions), all direct or indirect activity or facilitation, including financial transactions, are prohibited. Comprehensive Sanctions are often used in conjunction with Selective Sanctions and List-Based Sanctions. Currently, only the US utilizes Comprehensive Sanctions. Other sanctions authorities such as the UN, EU, and UK utilize targeted sanctions that prohibit certain activities such as investments in target jurisdictions. Sanctions from jurisdictions such as the EU, UK, and Canada also prohibit certain activities involving "Non-Government Controlled Areas" of Ukraine, including the Donetsk, Luhansk, Kherson, and Zaporizhzhia oblasts, although these sanctions are not comprehensive in nature.

Sensitive Sanctioned Countries ("SSCs")
● Cuba ● North Korea ● Iran ● The regions of Crimea, the so-called Donetsk People's Republic and the so-called Luhansk People's Republic

B. Selective Sanctions

Selective Sanctions tend to be more complex and nuanced and seek to prohibit a specific activity connected to a certain jurisdiction, industry sector or specific parties that are listed on a sanctions list. Selective Sanctions do not ordinarily require blocking or freezing of assets, but rather prohibit engaging in the prohibited activity, such as restricting the ability to access financing or exporting, importing, or providing certain goods, technology or services. While some Selective Sanctions incorporate List-Based Sanctions, which makes them easier to follow, other Selective Sanctions are not based on any list and require Binance to adopt targeted controls. For example, EU regulations prohibit providing crypto-asset wallet, account or custody services to Russian and Belarusian nationals and residents (unless they qualify as EU Persons as defined below) and entities established in Russia or Belarus (regardless of where its operations are located). Other examples of Selective Sanctions include "sectoral sanctions" that prohibit lending to, or dealing in debt or equity, of certain Russian and Belarusian entities.

C. List-Based Sanctions

List-Based Sanctions target Designated Persons and generally prohibit all activity with, on behalf of, or for the benefit of Designated Persons. List-Based Sanctions may also require blocking and/or freezing of the assets of Designated Persons. Examples of List-Based Sanctions include OFAC's Specially Designated

Nationals (“SDN”) List, the UN Sanctions List, the EU Sanctions List, and the UK Sanctions List, among others. These sanctions can be country related or activity based and target, for example, individuals and entities associated with governmental regimes that may threaten the stability of a country who are deemed to be involved in activities such as terrorism, terrorist financing, narcotics trafficking, transnational organized crime, human rights abuses and nuclear proliferation. List-Based Sanctions requirements may also apply to entities that are owned or controlled by Designated Persons on a Global Sanctions List or, where applicable, a Local Sanctions List, even if the entities are not separately listed. Binance entities must block/freeze property of Designated Persons on a Global Sanctions List or, where applicable, a Local Sanctions List and make reports to the relevant sanctions authorities according to applicable laws and regulations in the jurisdiction where they are registered, licensed, or operate.

Compliance with List-Based sanctions is achieved, primarily, by screening against published regulatory lists containing Designated Persons. Systems & Controls maintains and implements a full inventory of required lists that Binance uses for sanctions screening.

D. Customer Relationship Restrictions

Any customer relationship (or transaction) prohibited under this Policy must be immediately rejected/restricted and escalated to Global Sanctions. There may be limited circumstances when an exception to the Policy may be considered. All such requests must be submitted to Global Sanctions with the rationale for review and consideration.

(i) Customer Relationships - Designated Persons

The Binance Group must not enter into or maintain a relationship with a customer who is a Designated Person on a Global Sanctions List or, where applicable, a Local Sanctions List. Any accounts identified with a potential true match for such Designated Person must be immediately blocked/frozen and escalated to Global Sanctions.

(ii) Customer Relationships - SSCs

SSC Restrictions - Relationships	
An individual customer whose **residential address** (including **current address, permanent address or correspondence address**) is in an **SSC**	Prohibited
An entity customer that has its registered office address (including **business address, correspondence address or its principal place of operations address**)[3]	Prohibited

[3] Where related parties of an entity customer are nationals/residents of an SSC but the entity customer itself is not incorporated/registered in an SSC, SEQ must be triggered for the entity customer and any “YES” response in the SEQ will be escalated and risk-assessed on a case-by-case basis. Refer to section 2.1 above.

(iii) Customer Relationships - Selective Sanctions

Certain restrictions apply to customers with a nexus to a country subject to Selective Sanctions (e.g., Belarus, Russia and Venezuela), which are defined below.

Selective Sanctions Restrictions - Relationships		
Country	**Individual Customer Relationship**	**Entity Customer Relationship**
Russia / Belarus (Binance Entity's Operations in Non-EU Member States)	Permitted unless (1) the customer is a Designated Person or employed by/acting on behalf of the Government of Russia / Belarus, or (2) where a Binance entity relies on EU infrastructure or an EU service provider to provide crypto-asset wallet, account, or custody services to its customers (including Russian / Belarusian nationals and residents).	Permitted unless (1) the customer is a Designated Person; (2) the customer is owned 50% or more or controlled by a Designated Person or the Government of Russia / Belarus, or (3) where a Binance entity relies on EU infrastructure or an EU service provider to provide crypto-asset wallet, account, or custody services to its customers (including Russian / Belarusian nationals and residents).
Russia / Belarus (Binance Entity's Operations in EU Member States)	**Prohibited:** ● Russian / Belarusian nationals[1], unless they qualify as EU Persons[2] ● Any natural person residing in Russia / Belarus, unless they qualify as EU Persons ● Designated Persons ● Persons employed by/acting on behalf of the Government of Russia / Belarus	**Prohibited:** ● Entities established in Russia / Belarus, regardless of where its operations are located ● Designated Persons ● Entities owned 50% or more or controlled by a Designated Person or the Government of Russia / Belarus ● An entity (or legal body) established under the law of an EU Member state providing crypto-asset wallet, account or custody services, that is directly or indirectly owned or controlled, or that has any governing bodies with any posts, which are held, by any Russian / Belarusian national(s) or resident(s), unless each of those persons qualifies as an EU Person (this prohibition in respect of Belarus will be effective from 26 March 2025) Any entity customers established in the EU with UBOs that are Russian nationals or residents and fall under certain parameters stipulated in the Standard Operating Procedure for handling RU/BY Related Parties should be escalated to Global Sanctions for review and assessment on a case by case basis. A similar approach will be adopted in respect of any entity customers established in the EU with UBOs that are Belarusian nationals or residents.
Venezuela	Permitted unless the customer is a Designated Person, employed by or acting on behalf of the Government of Venezuela (a current official, employee or contractor of the Government of Venezuela), or a former	Permitted unless (1) the customer is or is owned 50% or more or controlled by a Designated Person; or (2) the customer is or is owned or controlled by

	official of the Government of Venezuela.	the Government of Venezuela.
	"Government of Venezuela" (as defined in Executive Order 13884) means the state and Government of Venezuela, any political subdivision, agency or instrumentality thereof, including the Central Bank of Venezuela and Petroleos de Venezuela, S.A. (PdVSA), any person owned or controlled, directly or indirectly, by the foregoing, and any person who has acted or purported to act directly or indirectly for or on behalf of, any of the foregoing, including as a member of the Maduro regime. This definition includes current or former government officials and current employees or contractors of the Government of Venezuela and state-owned enterprises.	

[1] Russian / Belarusian National is defined as any natural person who holds the citizenship of the Russian Federation or the Republic of Belarus in accordance with its legislation (wherever that person may be located /domiciled).

[2] EU Person is defined as nationals of an EU Member State, of an EEA country or of Switzerland, or natural persons having a temporary or permanent residence permit in one of those jurisdictions.

E. Transaction Restrictions

(i) Direct Exposure

Examples of direct exposure include:

- Transactions involving an SSC or Designated Person that are conducted through Binance accounts, products or services
- Investments or assets held by a customer involving an SSC or Designated Person that is prohibited under this Policy, where the proceeds or income from such investments are processed through Binance accounts, products or services
- Any activity, direct or indirect, involving an SSC or Designated Person that is prohibited under this Policy, where proceeds or income are processed through Binance accounts, products or services

Transaction Restrictions - Designated Person	
Individual/Entity	**Direct Exposure**
On a Global Sanctions List or, where applicable, Local Sanctions List	Prohibited

Transaction Restrictions - SSCs*	
SSC	**Direct Exposure**
Cuba	Prohibited
Iran	Prohibited
North Korea	Prohibited
The regions of Crimea, the so-called Donetsk People's Republic and the so-called Luhansk People's Republic	Prohibited

* Under limited circumstances, a **pre-approval** by Global Sanctions via TSE prior to transactions could be granted on an exceptional basis in respect of transactions involving SSCs. Such pre-approval could be provided, for example, in cases where such transactions would not be prohibited if they were undertaken by US persons.

Transaction Restrictions - Selective Sanctions**	
Country	**Direct Exposure[1]**
Belarus	In addition to List-Based Sanctions, Belarus is subject to a number of selective trade restrictions, including targeted restrictions on certain transactions involving the Government of Belarus and certain economic sectors. Belarus is not an SSC and is not subject to comprehensive sanctions. While it is permitted to have Belarusian nationals and residents as users, the BGSP prohibits facilitating activities that are prohibited by applicable Selective Sanctions. To identify such activities, enhanced sanctions due diligence is required for KYB users identified as having business exposure to Belarus (e.g., activities in the economic sectors listed below or exports of goods or services listed below) or to the Government of Belarus. Enhanced sanctions due diligence is also required for KYC users who indicate that they will use Binance's platform in connection with transactions involving the Government of Belarus, activities in the economic sectors listed below, or exports of goods or services listed below. Relevant economic sectors of the Belarus economy are listed below: 1. defense and related material 2. security 3. potassium chloride (potash) 4. tobacco products 5. construction 6. transport 7. energy 8. mining and quarrying sector 9. financial services Exports of relevant goods or services to Belarus are listed below: 1. financial assistance or services 2. professional services (e.g., IT, marketing, legal, accounting, consultancy services) 3. firearms 4. dual-use goods requiring an export license 5. aviation goods and technology 6. luxury goods 7. diamonds, gold, and mineral products 8. iron and steel Guidance on the required due diligence measures should be sought from Global Sanctions (via SanctionsAdvisoryBot). Upon receiving a request for guidance, Global Sanctions will advise on the enhanced due diligence steps required and, based on the information received, any applicable transactions restrictions.
Russia / Ukraine Programme* (All Binance Entities)	In addition to List-Based Sanctions, Russia is subject to a wide range of selective financial and trade restrictions, including targeted restrictions on certain transactions involving Russian state-owned entities and certain economic sectors. Russia is not an SSC and is not subject to comprehensive sanctions. However, the BGSP prohibits facilitating activities that are prohibited by applicable Selective Sanctions. To identify such activities, enhanced sanctions due diligence is required for KYB users identified as having business exposure to Russia (e.g., activities in the economic sectors listed below or exports of goods or services listed below) or to Russian state-owned entities.

Transaction Restrictions - Selective Sanctions**	
Country	**Direct Exposure[1]**
	Enhanced sanctions due diligence is also required for KYC users who indicate that they will use Binance's platform in connection with transactions involving the Government of Russia, activities in the economic sectors listed below, or exports of goods or services listed below. Relevant economic sectors of the Russian economy are listed below: 1. financial services 2. aerospace 3. marine 4. maritime oil and related 5. electronics 6. accounting 7. trust and corporate formation 8. management consulting 9. defense & technology (including quantum computing) 10. metals and mining 11. quarrying 12. architecture 13. engineering 14. construction 15. manufacturing 16. transportation 17. energy 18. media 19. gold Exports of relevant goods or services to Russia are listed below: 1. transactions with Russian stated-owned entities, 2. investments and/or projects in Russia and in non-government controlled areas in Ukraine (i.e., Crimea and the Donetsk, Luhansk, Kherson, and Zaporizhzhia oblasts) 3. financial assistance or financial services 4. warranting services for Russian-origin aluminum, copper or nickel 5. credit rating services 6. professional and business services (e.g., accounting, auditing, bookkeeping, tax consulting, legal advisory, IT consultancy, public relations, advertising) to the Russian government or entities established in Russia 7. supply of certain software (specifically for the management of enterprises and for industrial design and manufacture) to the Russian government or entities established in Russia 8. IP registration 9. dual-use items and common high priority items requiring an export license 10. firearms 11. luxury goods 12. diamonds 13. iron and steel products Guidance on the required due diligence measures should be sought from Global Sanctions (via SanctionsAdvisoryBot). Upon receiving a request for guidance, Global Sanctions will advise on the enhanced due diligence steps required and, based on the information received, any applicable transactions restrictions.

Transaction Restrictions - Selective Sanctions**	
Country	**Direct Exposure[1]**
Russian / Ukraine / Belarus Programme (Operations in EU Member States)	In addition to global prohibitions listed above, it is prohibited to provide crypto-asset wallet, account, or custody services from the EU or by an EU person to: ● Russian / Belarusian nationals, unless they qualify as EU Persons[2] ● Individuals residing in Russia / Belarus, unless they qualify as EU Persons[2] ● Entities established in Russia / Belarus, regardless of where its operations are located It is prohibited for EU persons or persons operating within the EU to directly or indirectly engage in any transaction with a credit or financial institution established outside of the EU or ***an entity providing crypto assets services*** that: ● are involved in transactions that facilitate, directly or indirectly the export, sale, supply, transfer or transport to Russia of specified dual-use goods and technology, goods or technology, common high priority items, and firearms and ammunition that are identified under the EU regulations; ● are involved in frustrating the prohibitions against providing financial support set out in Article 3s (of Regulation (EU) No 833/2014) concerning designated sanctioned vessels; ● circumvent the prohibition set out in Article 3n (of Regulation (EU) No 833/2014) concerning the provision of technical assistance, brokering services or financing or financial assistance, related to the trading, brokering or transport, including through ship-to-ship transfers, to third countries of Russian-origin crude oil or petroleum products.
Venezuela	All transactions involving the Government of Venezuela are prohibited. All cases involving the Government of Venezuela should be escalated to Global Sanctions (via SanctionsAdvisoryBot).

[1] Many of the sanctions provisions are executed through listing/designating parties on various regulatory lists, which include freezing and reporting obligations. It is important to be cognizant of potential indirect sanctions nexus where transactions are routed through other parties or overly complex in order to evade sanctions. There may also be licenses or wind down provisions in legislation permitting certain activity.

[2] EU Person is defined as a National of an EU Member State, of an EEA country or of Switzerland, or natural persons having a temporary or permanent residence permit in one of those jurisdictions.

** If there is any doubt whether an activity is permissible, the matter should be escalated to Global Sanctions.

(ii) Transaction Sanctions Exception ("TSE")

A transaction or activity prohibited by the BGSP requires an approved TSE before the transaction or activity can be processed or entered into.

TSEs will only be permitted where:

- the transaction is supported by a valid license issued by a relevant sanctions authority or is otherwise not prohibited under applicable sanctions laws and regulations, and
- there is no reason to believe the processing of the transaction will expose Binance to adverse publicity or reputational concerns. An example of an acceptable transaction includes, but is not limited to, a transaction in support of humanitarian aid, or an official request from a regulatory or law enforcement agency.

Certain transactions (where not prohibited under applicable sanctions laws and regulations) don't require an approved TSE:

- Interest credited by a Binance Entity
- internal transfers between the same name Blocked/Restricted Account
- Internal Binance charges and fees

TSE Approvals

Requests for a TSE approval must be submitted to Global Sanctions, for consideration, by providing details of the proposed transaction, rationale for the exception and a copy of the license issued to the customer, where applicable. Global Sanctions must keep a tracker of all TSE requests. TSEs need to be reviewed and/or re-approved annually if they cover an ongoing relationship.

Appendix II: Key Roles & Responsibilities

Role	Responsibilities[1]
Board of Directors ("Board")	The Board responsibilities include: ● Leadership of the Binance Group and setting the standards within the Group ● Approval of the Group's strategic objectives ● Oversight of the Group's operations ensuring competent and prudent management, sound planning, maintenance of sound management and internal control systems, adequate accounting and other records and compliance with statutory and regulatory obligations ● Key risk policies ● Extension of the Group's activities into new products or business or geographic areas outs of the agreed strategy approved by the Board
Audit and Finance Committee ("AFC")	The Binance Board of Directors (the "Board") established the AFC to: ● Assist the Board in fulfilling its supervision and oversight responsibilities relating to - ○ Binances' financial statements and other financial information ○ External and internal accounting and financial controls and processes ○ The qualifications, independence and performance of Binance's independent auditors ○ Design, implementation and performance of Binance's internal audit function ○ Treasury and finance matters ○ Auditing, accounting and financial report processes ● Serve as a focal point for communication between other directors, external and internal audit teams regarding their duties relating to financial and other reporting , internal controls, external and internal audits, and other matters as the Board determines.
Risk and Compliance Committee of the Board of Directors ("RCC")	The RCC was established by the Binance Board of Directors (the "Board") is assist the Board in fulfilling its supervision and oversight responsibilities relating to: ● Handling risk and compliance-related matters, including risk management and compliance controls ● Defining risk matrix and making recommendations on the risk appetite, profile and tolerance of Binance ● Risk management and compliance frameworks, policies and systems of Binance and overseeing the execution ● Compliance by Binance with legal and regulatory requirements
Chief Executive Officer ("CEO)	● Reports to the Binance Board ● Provide effective leadership supporting execution of this Policy by communicating and committing to a strong compliance culture emphasizing the importance of complying with the Policy and related procedures, and the consequences of non-compliance. ● Ensure appropriate and effective documented policies and procedures are implemented to support compliance with this Policy and applicable sanctions legislation ● Ensure adequate resourcing
Chief Operating Officer ("COO")	● Drive the requirements for the operation systems and controls to support compliance with the BGSP, in particular prioritizing customer screening systems architecture to ensure comprehensive customer sanctions and CTF screening across Binance ● Ensures adequate procedures and controls are implemented in compliance with the BGSP
Global Chief Compliance Officer ("GCCO")	● Reports to the Binance Board ● Oversees the implementation, operation and consistency of regulatory compliance and financial crime compliance programs across all functions globally, including AML/CTF, Sanctions and AB&C
Global Head of Sanctions ("GHS")	● Reports to Head of Enterprise Compliance, who reports to the GCCO ● Serve as the functional owner for the setting, maintenance, annual review and implementation of the BGSP ● Establish and implement a robust sanctions control framework to ensure that appropriate processes, procedures and technical solutions are in place to satisfy this Policy's requirements ● Accountable for the scope, completion and maintenance of Binance's EWRA for sanctions

Role	Responsibilities[1]
Chief Security Officer	● Reports to CEO ● Responsible for internal audit function to assess the effectiveness of the overall sanctions program across Binance and tests whether the Policy and implemented procedures and control are being adhered to
Head of Enterprise Compliance	● Reports to GCCO ● Responsible for overseeing the Global AML/CTF, Sanctions and ABC programs, intelligence and investigations functions which includes review of sanctions and terrorist financing related investigations, real time transaction screening and post transaction monitoring
Country Level General Manager	● Support execution of the BGSP through strong communication and reinforcement of the importance of compliance with this Policy and related procedures and the consequences of non-compliance ● Implement and maintain appropriate and effective documented procedures and related internal controls to ensure compliance with this Policy ● Ensure adequate resources and prioritization to ensure effective implementation of processes in support of this policy ● Ensure local laws are adhered to and the escalation of any non-compliance to Global Sanctions
Country Money Laundering Reporting Officer (“MLRO”)	● Reports to the Global MLRO ● Responsible for AML/CTF, Sanctions and ABC in-country ● Oversees the implementation of, and ensures compliance with, the BGSP as well as all applicable location sanctions laws and legislation for all operations within their country. ● Manage and complete a Country Addendum, if required. ● Work with the business in-country to ensure there are adequate sanctions-related procedures and controls in place. ● Serve as sanctions risk steward by providing effective oversight of operational risk management activities through appropriate review and challenge in order to support compliance with this Policy.
Human Resources	● Coordinates resourcing hires including ensuring background and screening checks are performed. ● Implements performance and reward procedures to ensure appropriate action is triggered where non-compliant activities or Policy breaches occur.
Global Screening Steering Committee (“GSSC”)	● The GSSC is chaired by the GCCO. Its mandate is to provide governance to the Binance name screening processes including: ○ Approving screening solutions including vendors ○ Configuration settings including fuzzy logic name matching, alert triggers, and automated processes ○ Authority to agree the application of regulatory keyword lists used in screening for Sanctions, Anti-bribery & Corruption, and Counter Terrorist Financing Programmes ○ Authority to agree the application of non-regulatory keyword lists, including any internal watchlist, used in screening for the Anti-money Laundering Programme, and reputational risk.
Global Transaction Screening Committee (“GTSC”)	● The GTSC is chaired by the GCCO. Its mandate is to provide governance and oversight of risk mitigation controls associated with processing fiat and virtual currency transactions by Binance, specifically: ○ Transaction Screening - real time system driven risk based screening of incoming/outgoing transactions ○ Transaction Monitoring - post transaction rules based monitoring to identify potentially suspicious transaction behavior ○ Geolocation controls - IP Address detection controls to detect transactions originating from a restricted jurisdiction, and controls to monitor and/or restrict users who appear to be actively attempting to circumvent these controls.

[1] Key roles may delegate specific tasks within their remit, however, overall accountability and responsibility remains with the individual.

Appendix III: Recusals

Binance employees are recused, without further action, from participating in activities that are prohibited under sanctions laws applicable to them, due to their citizenship, residency, or location.

Where a Binance employee is recused from a particular matter, a decision regarding assignment of their responsibilities relating to that matter may not involve a Binance employee who is also prohibited from acting under the applicable sanctions. The decision regarding reassignment of responsibilities should be referred to another responsible Binance employee within the same function or business line, who is not subject to the applicable sanctions and who has the same or higher career band ranking as the recused person.

If a recused Binance employee is asked to provide further advice or guidance that may give rise to a breach of applicable sanctions, the recused Binance employee should direct the requestor to this recusal statement. The table below sets out the definitions of nationalities relating to relevant sanctions laws.

US / Canada / EU / UK Persons and Other Nationalities	
Term	**Description**
US Persons	• Binance employees who are US citizens and US permanent residents (including green card holders), wherever located, or employed by Binance.US • Binance entities incorporated in the US and their employees, wherever located • Binance entities located in the US even if not incorporated in the US, including US branches of non-US Binance entities • Binance employees located in the US, even if temporarily (i.e. business trip or holiday)
Canada Persons	• Binance employees who are nationals of Canada • Binance employees located within Canada, regardless of nationality
EU Persons	• Binance employees who are nationals of a member state of the European Union, irrespective of where their activities take place • Binance entities incorporated or constituted under the law of an EU member state • A Binance employee within the territory of the European Union, including EU air space, regardless of its nationality
UK Person	• Binance employees who are nationals of the UK, irrespective of where their activities take place • A Binance entity in or constituted under the law of any part of the UK, including their branches outside the UK, irrespective of where their activities take place • A Binance employee or legal entity where their activity takes place wholly or partly within the UK Territory.
Other Nationalities	• In general, sanctions laws apply to the nationals of the sanctioning country, entities established under the country's laws, and persons inside the country's territory. • For specific details, consult the national legislation of the relevant country.

US Sanctions Prohibitions on US Persons Involvement or Facilitation

US Persons anywhere in the world must comply with US sanctions. Unless otherwise permitted under US sanctions, US Persons are generally prohibited from any direct or indirect engagement in any agreement, transaction, business or other dealing with any person subject to OFAC blocking sanctions, comprehensively sanctioned territories, or other activities prohibited under OFAC regulations. US persons are also prohibited from approving, brokering, negotiating, guaranteeing, financing, or otherwise facilitating activities of non-US persons that would be prohibited if undertaken by a US person. Facilitation also includes referral of prohibited business opportunities by a US Person to a non-US person. All Binance employees who are US Persons must comply strictly with the US sanction prohibitions on US Persons.

The facilitation prohibition also restricts the type of advice or other guidance US Persons may provide with

regard to activities prohibited by OFAC, including advice on how to structure a transaction so as to avoid US sanctions. It is not permissible for US Persons to advise how to structure a transaction so as to avoid or evade US sanctions. Binance employees who are US Persons must not be requested or expected to provide advice or other guidance on transactions where a risk of facilitation exists. Note, however, that OFAC regulations permit US persons to provide legal and compliance advice concerning how US sanctions would apply to activities of non-US persons, even if those activities would be prohibited for a US person. For further guidance, contact Global Sanctions or Legal.

Persons from other jurisdictions may also be subject to similar prohibitions regarding any direct or indirect engagement in any agreement, transaction, business or other dealing with designated parties or facilitating prohibited activities. The above principles apply to all Binance employees in relation to activities that would be prohibited under the laws and regulations of their country of nationality, residency, or location