CRYPTROVIA

U.S. SANCTIONS COMPLIANCE MANUAL

DOCUMENT HISTORY AND APPROVAL

REV.	VERSION/COMMENT	DATE	APPROVAL
1	Initial release	December 8, 2023	

For more information, please contact Cryptrovia's SCO:

Niko Argeroplos (niko@polemarch.com or 410-978-9939)

TABLE OF CONTENTS

1.INTRODUCTION

1.1.Management Policy Statement

As one of the world's premier physically backed non-fungible token ("NFT") marketplaces, Cryptrovia may encounter certain transactions or counterparties that present a risk of a violation of U.S. economic sanctions laws and regulations, such as parties using cryptocurrencies and purchases of NFTs to evade U.S. sanctions restrictions.

It is our policy that all Cryptrovia activities comply with U.S. economic sanctions laws and regulations administered by the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC"), as well as all other applicable export laws and regulations.[1] To this end, Cryptrovia has established compliance policies and procedures, including this manual, periodic compliance training, and any other policies or procedures that may be created by Cryptrovia to implement its sanctions compliance program.

Compliance is vital to protect U.S. national security and foreign policy interests and to ensure that Cryptrovia remains a trusted business partner and responsible corporate citizen. Every Cryptrovia employee has an obligation to ensure that they are aware of the requirements of sanctions and related export laws and regulations that pertain to their responsibilities, engage in routine monitoring of compliance, and carry out their responsibilities in strict compliance with the requirements of such laws and regulations.

Breaches of these laws and regulations are treated as strict liability offenses, meaning that even mistakes can violate the rules, and violations may subject Cryptrovia and the individual(s) involved to substantial civil and criminal penalties (including fines and imprisonment). Cryptrovia strongly encourages employees to promptly report suspected violations or concerns; reporting any known or suspected violations in good faith will not adversely affect an employee. Failure to comply with these laws and regulations, report non-compliance, or detect non-compliance within one's area of management responsibility will result in appropriate discipline.

Cryptrovia personnel will at all times act in an honest and ethical manner, and we are committed to upholding the laws of the United States and to fostering an atmosphere of educated compliance among our employees. By acting consistently with the policies and procedures herein, we can each do our part to assure that Cryptrovia earns its reputation as a company with the highest integrity.[2]

---

[1] OFAC, 31 C.F.R. § 500, *et seq.* OFAC's regulations are available on its website at: http://www.treas.gov/ofac.

[2] A statement of management policy of compliance with U.S. sanctions and other export laws, to be reissued annually, is included at **Appendix 1**.

1.2. Purpose and Scope

This manual applies to all Cryptrovia personnel and focuses on U.S. sanctions and related export rules that apply to our company, specifically those U.S. laws regulating sales, transfers, and exports of NFTs, cryptocurrency or other digital or fiat currencies, and goods/commodities (*e.g.*, luxury watches, electronics, artwork, precious metals, gems). Note that while this manual primarily addresses compliance with U.S. sanctions laws and regulations, other export obligations that may impact a small subset of Cryptrovia's activities – specifically, U.S. export controls and antiboycott requirements – are covered in this manual as well.

The manual includes:

- An introduction to Cryptrovia's U.S. sanctions compliance program;
- An overview of U.S. sanctions and related laws and regulations;
- The general procedures that Cryptrovia personnel must follow;
- In **Appendix 1**, a statement of management policy of compliance with U.S. sanctions laws and regulations;
- In **Appendix 2**, a sanctions compliance manual acknowledgement form; and
- In **Appendix 3**, a vendor/customer sanctions certification form.

This manual may be supplemented with targeted work instructions, operating procedures, and/or checklists, as appropriate.

Keep in mind that this manual does not provide definitive legal advice; rather, it is intended as an informative resource to assist Cryptrovia personnel in analyzing typical sanctions issues, particularly for its sales and redemption activities. As required, the manual may be modified to reflect any changes in the company's business model or increased export activities, address additional compliance requirements, or specify additional internal processes and procedures. In all cases, all relevant Cryptrovia personnel will be furnished a copy of the manual, as revised, for retention, and will be trained on the contents of the manual.

1.3. Implementation of the Program

Cryptrovia's Sanctions Compliance Officer ("SCO") is charged with implementing and overseeing this program and manages the day-to-day operations of Cryptrovia's sanctions compliance program. Cryptrovia has named **Niko Argeroplos** as the SCO.

Any questions that arise concerning U.S. sanctions or related export laws and regulations must be referred to the SCO or such persons designated by the SCO to assist. If questions and concerns remain regarding a particular project or transaction, outside counsel may be consulted.

The SCO coordinates all aspects of the sanctions compliance program and works with the appropriate business areas and/or functional elements with specific compliance responsibilities to ensure implementation. The SCO has the authority to review and prevent any transaction/project from proceeding unless all of the necessary sanctions- and other export-related requirements are satisfactorily completed. Only the SCO has the authority to apply for U.S. government licenses on behalf of Cryptrovia or to engage in any other formal regulatory matter before the U.S. government. As noted above, the SCO will be responsible for the day-to-day implementation and oversight of the compliance program, specifically including:

- Reviewing transactions for compliance with sanctions and other export requirements, including all purchases of NFTs, redemption of NFTs, acquisition of commodities/ goods, projects, and proposals, as appropriate;
- Conducting or coordinating necessary due diligence of prospective suppliers/vendors, customers, and other partners, including screening such parties and reviewing and resolving potential "red flags";
- Developing an annual training plan and overseeing implementation;
- When/if necessary, applying for all licenses and conducting other necessary interaction with the U.S. government and foreign governments;
- Investigating and identifying root causes of potential violations, overseeing and implementing corrective actions, and coordinating any compliance/enforcement disclosures or actions (with the assistance of counsel, as needed);
- Exercising authority to stop transactions unless all regulatory requirements are fulfilled;
- Monitoring changes in U.S. sanctions and other applicable export laws and regulations and updating Cryptrovia's compliance program accordingly;
- Acting as a clearinghouse for employee questions and concerns related to sanctions and related compliance issues; and
- Maintaining centralized files of all required records.

2.OVERVIEW OF U.S. SANCTIONS AND RELATED LAWS AND REGULATIONS

OFAC administers trade embargoes and economic sanctions programs against certain countries, regions, groups, and individuals. U.S. sanctions restrictions apply to a wide range of activities that extend beyond financial transactions to almost any dealings with a sanctioned target, including provision or receipt of goods or services, transfers of digital currency, contracts, transfers of evidence of title or ownership, and other transactions. Given that sanctions programs follow U.S. foreign policy and national security priorities, countries, regions, and persons under

sanction are subject to change. For this reason, appropriate personnel must keep abreast of sanctions-related developments.

2.1. Comprehensive Country- and Region-Based Programs

The U.S. government administers comprehensive or near-comprehensive embargoes against the following countries/regions:

- **Cuba**
- **Iran**
- **North Korea**
- **Syria**
- **Crimea region of Ukraine**
- **So-called Donetsk People's Republic ("DNR") region of Ukraine**
- **So-called Luhansk People's Republic ("LNR") region of Ukraine**

These sanctions are designed to cut off virtually all commerce between the United States and the countries/regions listed above. Thus, generally, imports from, exports to, and facilitation[3] of transactions with sanctioned countries/regions are prohibited, although exceptions and general licenses (*e.g.*, general authorizations) are available for certain exchanges. In certain instances, restrictions may also apply to foreign-incorporated subsidiaries of U.S. companies.[4] The SCO should be consulted with any questions regarding a sanctioned country/region.

2.2. Targeted Sanctions Programs

The U.S. government also administers more limited sanctions programs against other countries and/or their governments; transactions with these countries should be reviewed on a case-by-case basis.

---

[3] Essentially, prohibited facilitation occurs when a U.S. person facilitates a transaction by a foreign party that it could not engage in itself due to sanctions laws and regulations. For example, if a U.S. parent company exercises day-to-day control over a foreign subsidiary, such as by approving contracts or agents or engaging in hiring or firing decisions, this potentially would raise facilitation concerns if the foreign subsidiary engaged in business with a sanctioned target. Another common example is referral; if a U.S. employee receives an email requesting goods in a sanctioned country, that U.S. employee generally cannot simply forward the order to a non-U.S. entity to fulfill.

[4] OFAC can assert jurisdiction over non-U.S. entities under several circumstances, including if they are owned or controlled by a U.S. person (*e.g.*, Cuba and Iran sanctions); cause a U.S. person to violate OFAC's sanctions regulations; deal in U.S. goods or engage in U.S. dollar transactions cleared by U.S. banks; or violate particular U.S. sanctions laws and regulations that apply to conduct by non-U.S. persons, such as by reexporting U.S.-origin items to certain sanctioned entities, evading U.S. sanctions on Syria or Iran, or being involved with Iran's weapons of mass destruction program. Further, under certain circumstances (*e.g.*, Iran, Russia, and North Korea sanctions programs), OFAC can apply "secondary" sanctions to foreign entities for engaging in certain transactions with sanctioned persons/countries, even if there is no U.S. nexus to the transaction.

For example, **Afghanistan** is not subject to an embargo, but the Taliban is currently designated as a Specially Designated Global Terrorist ("SDGT") and subject to comprehensive sanctions under U.S. law. However, OFAC issued General License 20 for Afghanistan, which permits nearly all transactions involving Afghanistan or governing institutions in Afghanistan. The general license is broad, although it does not authorize financial transfers to the Taliban, the Haqqani Network, any entity in which the Taliban or the Haqqani Network owns, directly or indirectly, a 50% or greater interest, or any blocked individual, other than for effecting the payment of taxes, fees, or import duties, or the purchase or receipt of permits, licenses, or public utility services, provided that such payments do not relate to luxury items or services.

The **Belarus** sanctions program covers several key state-owned entities, certain government entities (including the Belarus KGB) and officials, and a number of close associates of President Lukashenka. Apart from the blocking sanctions, OFAC's Belarus Directive 1 prohibits transactions in, the provision of financing for, or other dealings (in both the primary and secondary markets) by U.S. persons or within the United States in "new debt" (including extensions of credit/payment terms) with a maturity of greater than 90 days issued on or after December 2, 2021 by the Ministry of Finance of the Republic of Belarus or the Development Bank of the Republic of Belarus. Note that Belarus also is subject to stringent U.S. export controls that prohibit exports, reexports, and transfers of many commercial and dual-use commodities, software, and technology (including many low-level EAR99 items) to Belarus.

OFAC has instituted extensive, targeted sanctions on **Russia**, including restrictions aimed at its financial services, energy, and defense/intelligence sectors that prohibit certain types of transactions with designated entities without a license, as well as sovereign debt restrictions and bans on new investment, the provision of certain services, and imports of certain Russian-origin items. Additionally, many Russian individuals and entities, including major Russian financial institutions, are subject to blocking and/or sectoral sanctions. The U.S. government has imposed other measures against Russia as well, including potential penalties on persons that engage in a significant transaction with certain entities in Russia's defense or intelligence sector (https://www.state.gov/t/isn/caatsa/275116.htm), along with certain transactions related to energy export pipelines. Note that Russia also is subject to stringent U.S. export controls that prohibit exports, reexports, and transfers of many commercial and dual-use commodities, software, and technology (including many EAR99 items) to Russia.

Additionally, OFAC administers targeted restrictions on **Venezuela**, including financial restrictions and a ban on engaging in most business with the Venezuelan government (including state-owned entities) and certain sanctioned individuals/companies in Venezuela.

2.3. List-Based Programs

In addition, the U.S. government maintains lists of individuals, entities, organizations, and shipping vessels associated with terrorism, narcotics trafficking, proliferation of weapons of mass destruction, or other national security concerns. Generally, transactions with these persons, including imports, exports, and the provision of services, are prohibited or subject to restrictions

without a U.S. government license. OFAC primarily identifies such persons on its Specially Designated Nationals ("SDN") List, although OFAC administers other list-based programs as well. The U.S. Departments of Commerce and State also maintain lists of sanctioned/denied parties, many of which restrict export activities involving these parties. A consolidated list of U.S. government sanctioned and denied parties is available at: https://www.trade.gov/consolidated-screening-list.

Importantly, OFAC's sanctions (including the SDN sanctions described above) generally extend to any entity 50% or more directly or indirectly owned, in the aggregate, by sanctioned individuals or entities, even if such entity is not specifically designated as a sanctioned party.

2.4. Other Export-Related Laws and Regulations

This manual primarily addresses compliance with U.S. sanctions laws and regulations, which apply to all of the company's activities, including purchases, sales, redemptions, and other transactions. To the extent that Cryptrovia engages in export activities, such as the shipment of goods/commodities from the United States to a foreign country when its customers redeem NFTs, personnel must also ensure that the company is complying with U.S. export requirements. A summary of the key export-related restrictions that apply to our operations is provided below.

2.4.1. U.S. Export Controls

The U.S. Export Administration Regulations ("EAR"),[5] which are administered by the U.S. Department of Commerce's Bureau of Industry and Security ("BIS"), control the export, reexport, and transfer (in-country) of commercial and dual-use commodities, software, and technology, as well as certain less sensitive military and satellite-related items. The EAR's coverage is quite broad; these regulations apply to U.S.-origin items, items physically located in the United States, and certain foreign-made items that contain or were derived from U.S. content. Even purely commercial items (*e.g.*, the chair you are sitting in, watches, jewelry, precious metals) are subject to the EAR's controls, although typically a license is not required to export (*e.g.*, ship, electronically transmit, or hand-carry out of the United States) such items to most destinations.

The EAR's Commerce Control List ("CCL") identifies items subject to controls and assigns these items an Export Control Classification Number ("ECCN"). To determine whether a license is required to export a product or technology, exporters must: (1) identify the item's ECCN and the corresponding reasons for control; and (2) cross reference the reasons for control (such as National Security or "NS") with the Commerce Country Chart. Commercial items that are not listed on the CCL are given the designation "EAR99" (a basket category and the lowest level of control) and generally are eligible to be exported without a license to all countries other than sanctioned or restricted countries/regions, provided that Cryptrovia has confirmed that no

---

5 EAR, 15 C.F.R. § 730, *et seq*.

prohibited end-uses/-users[6] or sanctioned/denied persons are involved.

2.4.2. U.S. Antiboycott Restrictions

The U.S. Department of Commerce's Office of Antiboycott Compliance and the U.S. Department of the Treasury administer separate antiboycott laws and regulations, which were enacted in response to the Arab League's boycott of Israel but apply to all unsanctioned boycotts.[7] Cryptrovia must not participate in any economic boycott that is contrary to U.S. antiboycott laws and regulations. Cryptrovia will not provide boycott-related information or prohibited statements to any party and will report such requests to the U.S. government.[8]

Any agreements, letters of credit, shipping instructions, or other business documents that contain requests for information related to country of origin (*e.g.*, a request to certify that goods did not originate in a particular country, as opposed to a permissible request to simply state the country of origin of the product), business with boycotted countries, religion, race, nationality, or national origin must be referred to the SCO for review and resolution. Cryptrovia should be particularly alert to requests (in emails, contracts, purchase orders, redemption documents, etc.) referencing the following: boycotts or the boycott laws; Israel; the six-pointed star; a blacklist or ineligible persons; eligibility of vessels or other parties; certifications that products or services are not from Israel; race, religion, sex, or national origin; and past business relationships with or in Israel or with blacklisted companies. Importantly, even a boilerplate contractual clause requiring compliance with the general laws of a foreign country may be deemed an agreement to cooperate with a boycott if that country is on the Department of the Treasury's list of boycotting countries (currently, Iraq, Kuwait, Lebanon, Libya, Qatar, Saudi Arabia, Syria, and Yemen).

The U.S. Department of Commerce and the Department of the Treasury prohibit/penalize compliance with boycott requirements, and the U.S. government imposes certain reporting requirements for boycott requests and agreements as well as operations in boycotting countries, so any requests to participate in a boycott must be promptly reported to the SCO.

---

6 Specifically, an export license may be required for items (including EAR99 items) intended for certain nuclear, biological or chemical weapons, or missile proliferation end-uses. In certain cases, a license may be required for items for a military or military-intelligence end-use/end-user (*e.g.*, Belarus, Burma, Cambodia, China (including Hong Kong), Russia, Venezuela, and, in certain instances, Iraq), certain oil and gas projects in Russia, and certain supercomputer and semiconductor development and manufacturing end-uses in China (including Hong Kong and Macau). Some activities of U.S. persons related to weapons proliferation and military-intelligence end-uses/end-users, as well as certain semiconductor development and production in China (including Hong Kong and Macau), also are prohibited without a license.

7 These laws and regulations, like the other laws and regulations covered in this manual, can apply to foreign affiliates of U.S. companies as well.

8 Information regarding the Department of Commerce's antiboycott regulations is available at: http://www.bis.doc.gov/index.php/enforcement/oac. The Department of the Treasury's separate antiboycott law requires U.S. taxpayers to report "operations" in or related to boycotting countries and requests received and agreements made to participate in or cooperate with an international boycott in their annual tax returns. *See* Tax Reform Act of 1976, Pub. L. No. 94-455, 1061-64, 1066-67, 90 Stat. 1649-50, 1654 (1976); I.R.C. § 999.

2.5. Penalties

The U.S. government has broad discretion as to whether and how to impose penalties. Under most OFAC programs (as well as the related export regulations discussed above), civil penalties can range up to the greater of approximately $300,000 per violation (periodically adjusted for inflation) or twice the value of the transaction. Criminal penalties are also authorized and can apply to any person who willfully commits, willfully attempts to commit, willfully conspires to commit, or aids or abets in the commission of a violation of OFAC's regulations. Criminal penalties can include fines of up to $1,000,000 per violation and/or 20 years imprisonment.

3. GENERAL COMPLIANCE PROCEDURES

Below are general compliance procedures that Cryptrovia personnel must follow to ensure that the company complies with sanctions and other related requirements.

3.1. U.S. Sanctioned/Denied Party Screening and "Red Flags" Check

3.1.1. General Screening Requirements

All vendors, suppliers, banks, customers, contractors, brokers, freight forwarders, other shipping partners and vessels, distributors, agents, representatives, employees, and other partners (and their beneficial owners) must be screened against the countries/regions subject to comprehensive or near-comprehensive U.S. sanctions (currently, Cuba, Iran, North Korea, and Syria; and the Crimea, DNR, and LNR regions of Ukraine[9]), as well as the countries subject to targeted restrictions (currently, Afghanistan, Belarus, Russia, and Venezuela).

All such individuals and entities (and their beneficial owners) also shall be screened against the various U.S. government lists of sanctioned/denied parties. These lists include OFAC's SDN, as well as other lists of U.S. government denied parties such as BIS's Entity List. Cryptrovia contracts with Sum and Substance Ltd (UK), a third-party vendor that provides screening software that includes all of the U.S. sanctioned/denied parties lists relevant to Cryptrovia's business.

3.1.1.1. OFAC's "50% Rule"

As noted above, OFAC's sanctions generally apply to entities 50% or more directly or indirectly owned, in the aggregate, by sanctioned individuals or entities. Therefore, it is important to conduct due diligence on not only the prospective vendor, customer, or other partner, but also its direct and indirect owner(s) if the prospect is an entity/organization. This can include conducting public source and third-party research (*e.g.*, Dun & Bradstreet, Hoovers, Bloomberg Law,

---

[9] Following the imposition of comprehensive sanctions against certain regions of Ukraine, some companies located in the embargoed regions began to list their country of location as Russia in order to evade U.S. sanctions. Accordingly, screening of entities identifying their country of location as Russia or Ukraine should also involve screening city names and any other regional indicators to ensure that such companies are not subject to the comprehensive sanctions.

Cryptrovia's screening service), issuing prospective partners a short questionnaire on their ownership, and/or requiring them to certify that they are not owned by a sanctioned target. The certification/contractual language may also require the prospective partner to provide prompt written notification to Cryptrovia upon any change in ownership that could trigger any prohibitions on U.S. persons engaging in transactions with the entity. A sample certification form is included at **Appendix 3**.

3.1.1.2.SDN Officials, Executives, and Employees

Even if a vendor, customer, or other partner is not a sanctioned party, OFAC generally prohibits engaging in any dealings with an SDN working for or overseeing the company (*e.g.*, an SDN CEO or SDN employee). Per OFAC guidance, activities such as negotiating with an SDN or signing a contract with a company where the SDN is the signatory are prohibited. Accordingly, to the extent there will be any direct interactions with specific individuals working for a vendor, customer, or other partner, Cryptrovia will also screen the names of the individuals with whom it will be dealing.

3.1.2.When to Screen and Responsible Groups

Screening will be overseen by the SCO and performed by the SCO or a designee using the company's third-party screening software. For each type of transaction below, personnel must follow the Screening Work Instructions available at https://sumsub.com/guides-reports/transaction-monitoring-tactics-preventing-fraud-and-achieving-aml-excellence/, which detail how to utilize our screening software and perform the screening function.

3.1.2.1.Point of Sale of the NFT

Prior to selling NFTs valued at $10,000 or less, Cryptrovia will collect the prospective customer's full legal name, digital wallet address information and IP address, and email address and screen this information to ensure that there is no link to sanctioned individuals or entities, hacks or exploits, or other illegal activity.

Prospective customers purchasing more than $10,000 worth of NFTs in a 24-hour period will be required to provide additional information, including physical address, date of birth (as applicable), and nationality, and will be subject to enhanced due diligence and screening.

3.1.2.2.Sellers/Vendors

All new vendors must apply to be a Cryptrovia seller and undergo an onboarding process that includes due diligence and screening. Among other information, Cryptrovia will collect and screen each new vendor's full legal name, trade name (if applicable), physical address, and email address. For vendors that are entities, Cryptrovia also will conduct ownership diligence to ensure that the vendor is not owned by any sanctioned parties.

3.1.2.3.Redemption of NFTs

Prior to redeeming NFTs, Cryptrovia will collect and screen the legal name, trade name (if applicable), physical/shipping addresses, wallet address, and IP address of the customer. Although most customers are individuals, Cryptrovia will conduct ownership diligence on any entities seeking to redeem NFTs to ensure that they are not owned by sanctioned parties.

3.1.2.4.Ongoing Monitoring

As appropriate, the parties identified above (*e.g.*, vendors/sellers) will be periodically re-screened, such as during any agreement renewal or reactivation or if the party undergoes a material change in ownership, as U.S. restrictions are continuously updated.

3.1.3.Geolocation Tools and IP Blocking

To help ensure that users from embargoed countries and regions cannot access the company's services, Cryptrovia employs tools to identify and block IP addresses and wallets from embargoed countries/regions, along with analytic tools that can identify IP misattribution.

3.1.4.Identifying "Red Flags"

Personnel also should be alert to any "red flags" or unusual circumstances suggesting a potential violation of U.S. sanctions or related laws and regulations. Such "red flags" could include, for example, a person with a wallet or physical address similar to a U.S. sanctioned/denied party, information in an email address or other identifying information suggesting that a person may be located in an embargoed country or region, or a person who wants to use abnormal shipping terms. Overall, it is critical that Cryptrovia does not cut off the flow of information that comes to it in the normal course of business and fully investigates and resolves any "red flags."

3.1.5.Screening Results and Escalation

To the extent there are no potential positive hits to a sanctioned/denied party, a country/region subject to sanctions is not involved, and no "red flags" are present, the transaction can be processed, subject to the additional requirements outlined in Section 3.3 for export activities.

If there is an exact hit, potential positive match, country/region subject to an embargo or targeted sanctions, or "red flag" – such as a name that matches or is very similar to a sanctioned party or an email address with a top-line domain associated with a sanctioned jurisdiction – the transaction must immediately be put on hold and cannot be processed unless and until approved by the SCO or a designee. All positive or possible positive matches to sanctioned/denied individuals, entities, countries, or regions, as well as any "red flags," must be promptly reported to and reviewed by the SCO or a designee. The SCO or a designee may collect additional information to confirm a positive or false positive match and escalate the issue, including to outside counsel, if necessary. The SCO or a designee will either clear the transaction and notify

relevant personnel that the transaction may proceed or notify such personnel that the transaction cannot proceed and discuss next steps (*i.e.,* whether to apply for a specific license to engage in the transaction, whether reporting requirements apply, etc.). Under no circumstance may a suspended transaction proceed until a determination has been made by the SCO or a designee that the party involved is not subject to U.S. sanctions or related restrictions.

3.2. Blocked and Rejected Transaction Reporting

To the extent Cryptrovia's transaction screening and monitoring triggers a valid positive match to a sanctioned party, country, or region, Cryptrovia also may be required to submit a blocked property report (*e.g.*, if an SDN is involved) or a rejected transaction report (for transactions rejected for sanctions reasons that do not involve an SDN/blocked property) to OFAC. The SCO or a designee will coordinate with outside counsel as needed and file any required reports, which must be submitted within 10 business days. The SCO or a designee also will file an annual report reflecting all currently held blocked property, by September 30 each year, as required.[10]

3.3. Additional Requirements for Export Activities

If Cryptrovia engages in export activities, such as the shipment of goods/commodities by the company or via a third-party distributor from the United States to a foreign country after customers redeem NFTs, personnel must also ensure that the company is complying with all other applicable U.S. export requirements. Any questions regarding these restrictions must be escalated to the SCO or a designee, who may consult with outside counsel as necessary.

3.3.1. Export Controls and Export Reporting

For goods/commodities sourced by Cryptrovia from its vendors that may be exported upon redemption of NFTs, Cryptrovia will request and maintain a record of the ECCN or EAR99 designation of the items from the supplier/vendor, as appropriate.[11] To the extent an item is classified under an ECCN on the CCL, Cryptrovia's SCO, with the assistance of outside counsel as necessary, will ensure that the item is appropriately authorized for export to the ultimate destination. Even for items classified as EAR99 for export control purposes (the U.S. export classification that will apply to most items provided by Cryptrovia), Cryptrovia still must ensure that no sanctioned/denied parties or countries/regions are involved in the transaction and that its items will not be provided to/for prohibited end-uses or -users under U.S. law, such as weapons proliferation end-uses or military-intelligence end-users/-uses in certain countries. As noted above, countries subject to targeted sanctions must be reviewed on a case-by-case basis; many

---

[10] OFAC's reporting forms and delivery instructions are available here: https://home.treasury.gov/policy-issues/financial-sanctions/ofac-reporting-system.

[11] Cryptrovia will **not** export or otherwise deal in defense/munitions items controlled by the U.S. International Traffic in Arms Regulations ("ITAR"), or any firearms, ammunition, explosives, or other items controlled by the Bureau of Alcohol, Tobacco, Firearms and Explosives ("ATF").

luxury and other goods, for example, cannot be directly or indirectly exported from the United States to Russia or Belarus.

Any third-party distributors shipping items abroad on Cryptrovia's behalf must receive an alert/notice from Cryptrovia prior to releasing such shipments; this alert/notice can only be issued by Cryptrovia after it has completed its screening and export licensing review.

Cryptrovia personnel also should be alert to and investigate any pre- or post-shipment "red flags." Additionally, Cryptrovia will ensure that the company, its freight forwarder, and any third-party distributors comply with all applicable export clearance requirements, such as the filing of Electronic Export Information ("EEI")/trade data[12] and inclusion of required destination control statements on the shipping paperwork.[13]

3.3.2. Antiboycott Screening

Employees must be alert to and report any requests to comply with an unsanctioned boycott to the SCO, who will manage all antiboycott-related reporting requirements and may consult outside counsel as necessary. Examples of boycott-related requests are provided above. EAR-related boycott requests should be reported to BIS electronically or using Form BIS-621P (single transaction) or Form BIS-6051-P (multiple transactions).[14] Reports of "operations" in or related to boycotting countries (as defined by Treasury) and requests received and agreements made to participate in or cooperate with an international boycott must be reported using IRS Form 5713 in Cryptrovia's annual tax return.

---

12 Many physical (tangible) export shipments require submission of EEI in the Automated Export System ("AES"), including most shipments where the value of the commodities classified under an individual Schedule B number or Harmonized Tariff Schedule ("HTS") commodity classification code exceeds $2,500. In other cases, EEI exemptions may apply; these exemptions are transaction-specific, do not apply to certain types of transactions (*e.g.*, licensed shipments), and must be annotated on certain documentation. *See* Foreign Trade Regulations, 15 C.F.R. Part 30; *see also* 15 C.F.R. Part 758.

13 For example, the EAR generally require that the following destination control statement be included as an integral part of the commercial invoice when items classified above EAR99 (*i.e.*, items with an ECCN) are shipped abroad in tangible form:

> ***These items are controlled by the U.S. government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations.***

14 These reporting forms are available on BIS's webpage at: http://www.bis.doc.gov/index.php/enforcement/oac. Where the person receiving the request is located in the United States, each report must be postmarked or electronically date-stamped by the last day of the month following the calendar quarter in which the request was received (*e.g.*, April 30 for the first quarter). Where the person receiving the request is located outside of the United States, each report must be postmarked or electronically date-stamped by the last day of the second month following the calendar quarter in which the request was received.

3.4. Training and Awareness

The SCO must ensure that all relevant employees, including senior management, have received training appropriate to each person's areas of responsibility and sufficiently addressing compliance with sanctions regulations, including the vetting procedures described above, and other applicable export requirements. As appropriate, new employees must receive training soon after beginning employment. The SCO or a designee will document these training sessions, including a list of the participants, and completion of such training will be considered in performance reviews. A training schedule also must be implemented so that relevant employees are provided routine updates and refresher courses, as appropriate.

Employees involved in activities that may implicate sanctions or related requirements must receive periodic job-specific, intermediate, and/or advanced training. The ECO and any designees are required to receive detailed, periodic training on U.S. sanctions and other export regulations that could impact Cryptrovia's operations, including through outside programs.

In addition to formal training, the SCO may issue alerts or updates to inform employees of important changes in U.S. laws and regulations or to remind employees of certain key compliance obligations.

3.5. Compliance Language

To the extent feasible, contracts, terms of service, and related documents will include standard language requiring Cryptrovia's partner to comply with U.S. economic sanctions laws and regulations and all other applicable U.S. export laws and regulations.

3.6. Due Diligence and Merger & Acquisitions

Before entering into any business transactions, Cryptrovia personnel (with the assistance of outside counsel, as necessary) must investigate and conduct due diligence on the party with whom the transaction will be taking place, particularly when engaging in the acquisition of another company or assets. Sanctions and export compliance due diligence in the mergers and acquisitions context is critical because Cryptrovia can inherit liability for any violations by the target company, especially if the transaction involves traditional share transfers or a merger. Post-transaction, the SCO or a designee will conduct additional diligence and testing/auditing as needed and ensure that all newly acquired companies/assets are promptly integrated into Cryptrovia's compliance program.

3.7. Risk Assessment Function

The SCO or a designee must routinely assess and identify new risk areas, including when there are material changes to Cryptrovia's operations (*e.g.*, opening a new office, engaging in business in a new country, changes in customer base or supply chain, dealings in new types of commodities), and modify the company's policies and procedures accordingly. As appropriate,

additional training will be provided to address and mitigate any new risk areas.

3.8. Auditing and Testing

Cryptrovia will verify the effectiveness of its compliance program, both through formal audits (conducted by internal or external auditors, as appropriate) and more frequent "spot checks" (conducted by the SCO or a designee). As necessary, findings and recommendations will be developed following each review, and the SCO and senior management shall take appropriate action where it appears that a potential violation may have occurred. The SCO will be responsible for developing and managing corrective actions to address the findings and recommendations of any review. When appropriate, additional training will be provided to address any identified weaknesses.

3.9. Reporting and Investigating Potential Violations

Cryptrovia employees are encouraged to notify their supervisor, the SCO, or senior management of any suspected violation of U.S. economic sanctions laws and regulations or other export requirements. The SCO must ensure that there is a centralized reporting structure for potential violations and will publicize avenues for employees to report potential violations, including a mechanism for anonymous reporting. No employee will be adversely affected or retaliated against for reporting non-frivolous concerns.

The SCO or a designee will promptly investigate suspected violations, determine root causes of any apparent violations, and, in conjunction with senior management, determine any corrective or remedial actions, including disclosure of potential violations to the relevant U.S. government authorities. Senior management's response, as well as the implementation and status of corrective actions, will be documented, and the SCO will report back to senior management upon completion of the corrective actions.

3.10. Responding to External Reports of Non-Compliance

Periodically, third parties such as government agencies or payment processors may apprise Cryptrovia of potential positive matches from their own screening efforts or other sanctions risks. Any such communication must be immediately reported to the SCO, who will act as the point of contact with the third parties. Cryptrovia will promptly address third-party inquiries, and any gaps in Cryptrovia's sanctions compliance processes or potential violations will be handled in accordance with Sections 3.8 and 3.9 above.

3.11. Records Retention Policy

Documents relating to sanctions or other export issues – such as screening results and resolutions, compliance training records, audit results, and shipment records – shall be maintained for at least five years from the date of the transaction/shipment, the date of the cessation of work, or the expiration of an applicable U.S. government license, whichever is

longer. The SCO will work with IT personnel to ensure that Cryptrovia's corporate document retention requirements and document deletion schedule comply with these requirements.

These records must be complete, readily and easily accessible, readable and legible, backed up, and able to be reproduced in paper form. Cryptrovia's records system also must preserve and prevent the initial images from being altered and record all changes to the original records (including by whom and when). Additionally, Cryptrovia personnel at all times will have procedures in place that identify the individuals who are responsible for the operation, use, and maintenance of the system, as well as inspection and quality assurance procedures.

Appendix 1
Statement of Management Policy of Compliance with U.S. Sanctions Laws

MEMORANDUM

TO: **All Personnel**

FROM: Nikephoros Argeroplos
DATE: December 8, 2023 - To be reissued and published annually
RE: **Policy of Compliance with U.S. Sanctions Laws**

It is the policy of Cryptrovia that all of its activities will fully comply with the economic sanctions laws and regulations of the United States, including all regulations implemented by the U.S. Department of the Treasury's Office of Foreign Assets Control, as well as other applicable export laws and regulations.

Compliance is vital to protect the national security and foreign policy interests of the United States. Every Cryptrovia employee has an obligation to ensure that they are aware of the requirements of sanctions and other export laws and regulations that pertain to their responsibilities, engage in routine monitoring of compliance, and carry out their responsibilities in compliance with the requirements of such laws and regulations.

Strict compliance with Cryptrovia's prescribed sanctions compliance procedures at all times is the only acceptable standard of behavior. Any deviation from this standard, even through ignorance or carelessness, is a serious matter and will result in appropriate discipline, up to and including termination of employment. Failure to report non-compliance or to detect non-compliance within one's area of management responsibility will result in appropriate discipline. Violations of these laws also may subject Cryptrovia and the individual involved to substantial civil and criminal penalties.

Our Sanctions Compliance Officer will supervise the U.S. sanctions compliance program and serve as the principal contact for sanctions- and export-related matters.

As a responsible corporate citizen, we are committed to upholding the laws of the United States and to fostering an atmosphere of educated compliance among our employees. I cannot stress enough the importance of complying with U.S. sanctions laws and other applicable export requirements. Your strict adherence to Cryptrovia's compliance program is essential to Cryptrovia's continued growth and its continued standing as a responsible corporate citizen.

Appendix 2
Sanctions Compliance Manual Acknowledgement Form

Instructions: After reading Cryptrovia's U.S. Sanctions Compliance Manual, please review and submit this signed certification to the Sanctions Compliance Officer. If you are unable to attest to the truth of one or more of the statements below, please promptly contact the Sanctions Compliance Officer.

I, Nikephoros Argeroplos, hereby acknowledge and certify that I have reviewed and understand Cryptrovia's U.S. Sanctions Compliance Manual. I understand my responsibilities to comply with: (1) all U.S. economic sanctions laws and regulations, including sanctions regulations administered by the Office of Foreign Assets Control, and all other applicable export laws and regulations; and (2) all Cryptrovia compliance policies and procedures.

I agree to fully comply with all applicable sanctions and export laws and regulations for the duration of my employment with Cryptrovia and understand and agree that failure to comply with such laws and regulations or with applicable Cryptrovia policies and procedures could result in personal liability, liability for the company, and disciplinary action up to and including termination of my employment.

I also understand that neither the U.S. Sanctions Compliance Manual nor any related training constitutes a legal opinion, and that case-by-case legal analysis is required for each compliance issue that may arise. If I have a question about sanctions or export compliance or Cryptrovia's policies, procedures, or legal obligations, I will consult with the Sanctions Compliance Officer.

Signature: _____

Name: Nikephoros Argeroplos

Date: December 8, 2023

Appendix 3
Vendor/Customer Certification

[INSERT ON VENDOR/CUSTOMER LETTERHEAD]

CERTIFICATION

[Insert vendor/customer name] hereby certifies that:

(1) it is not located, ordinarily resident, or headquartered in, nor directly or indirectly owned by any individuals or entities located, ordinarily resident, or headquartered in, (a) Cuba, Iran, North Korea, or Syria; (b) the Crimea, so-called Donetsk People's Republic ("DNR"), or so-called Luhansk People's Republic ("LNR") regions of Ukraine; or (c) any other country/region subject to comprehensive or near-comprehensive U.S. sanctions;

(2) it is not designated or otherwise identified on any of the various U.S. government lists of sanctioned/denied parties, including, but not limited to, the U.S. Department of the Treasury, Office of Foreign Assets Control's Specially Designated Nationals and Blocked Persons List, Sectoral Sanctions Identifications List, or Foreign Sanctions Evaders List; the U.S. Department of Commerce's Denied Persons List, Unverified List, or Entity List; the U.S. Department of State's AECA Debarred List or Non-Proliferation Sanctions Determinations; or other applicable U.S. Executive Orders;

(3) it is not 50% or more directly or indirectly owned, in the aggregate, by one or more individuals, entities, or governments sanctioned by the U.S. government; and

(4) it will provide prompt written notification to Cryptrovia of any change that may result in the company being subject to U.S. sanctions or other import/export restrictions or that otherwise may impact the representations above.

By signing this statement, I certify that all representations herein are true, correct, and complete to the best of my knowledge, and that I am a duly authorized representative of [Insert vendor/customer name] with the authority to make and sign certifications on behalf of [Insert vendor/customer name].

{company chop}

Signature: _____

Name: _____

Title: _____

Date: _____