

Crypto Risk Management Policy

SUNSTAR IMPACT N.V. (“Sunstar” or “the Company”)

1. Version Control

Name	Description
Document name	Crypto Risk Management Policy
Version	1
Author	Sunstar Impact N.V. - Compliance Department
Authorised By	Sunstar Impact N.V. - Board of Directors
Distribution Date	November 4, 2024
Security Classification	High

All rights reserved. The information contained in this Policy is confidential and the intellectual property of the Company and for use during the course of employment with the Company or other companies within the same group. It may not be relied upon by, or enclosed or circulated to, any other person or for any other purpose without the prior written consent of the Company.

2. Contents

1. Version Control
2. Policy Statement
3. Purpose and Scope
4. Key Risk Identification. Risk Mitigation Strategies
5. Roles and Responsibilities
6. Staff education, training and development
7. Version control

Policy Statement

The purpose of this Crypto Risk Management Policy (the "Policy") is to establish a comprehensive framework for identifying, assessing, managing, and mitigating the risks associated with the cryptocurrencies used by the Company. The Policy aims to ensure compliance with applicable legal and regulatory requirements, safeguard the Company's financial assets, and maintain the integrity of its gambling operations.

The Company is committed to ensuring robust and effective controls, measures and processes to identify gaps and risks, to have proportionate oversight functions and mitigate risk as much as possible.

This Policy states Company's risk management objectives and sets out its approach to managing and mitigating risks associated with crypto, as well as providing defined and detailed procedures for identification, assessment, mitigation and corrective actions. The Company is dedicated to ensuring that the responsible employees engaged with crypto transactions are fully trained and understand the implications of risk and know that its structured procedures, systems and controls have been put into place to identify the risks, mitigate where possible and prevent unnecessary harm or damage to the Company. Adherence to this Policy is mandatory and non-compliance could lead to disciplinary action.

Purpose and Scope

The purpose of this Policy is to provide Company's objectives, intent, approach and procedures for crypto risk management and assessment, and to act as a guidance document for employees and third parties. Effective risk management requires a robust and defined framework, detailing the functions, actions and controls used to identify, assess and prevent risks. To set out the policies, procedures, systems and controls necessary for the Company to meet its obligations, Company's approach shall be based upon:

- National Ordinance Identification when Rendering Services (NOIS)
- National Ordinance Reporting Unusual Transactions (NORUT)
- National Ordinance on the Supervision and Regulation of Games of Hazard (NOOGH)

Together referred to as "the codes" in relation to the detection and prevention of crypto risks.

The procedures that are appropriate for the purpose of forestalling and preventing crypto risks include:

- Identify the main risks associated with crypto payments.
- Assess/measure the importance, impact and likelihood of the risk.
- Mitigate the risks through corrective actions, controls and operational measures.
- Reassess the risk importance, impact and likelihood.
- Carry out ongoing monitoring of the risk and mitigating controls.

Key Risk Identification. Risk Mitigation Strategies

The Company identifies the following key risks associated with cryptocurrency in its online gambling operations:

1. Money Laundering and counter financing terrorism and Fraud Risk

Cryptocurrencies can be used to facilitate money laundering, fraud, and other illicit activities. The Company takes a zero-tolerance approach to money laundering, terrorist financing and other such financial crimes. The Company informs and helps educate staff and other stakeholders to understand Company's stance towards these issues.

It is Company's policy that:

- Statutory and regulatory obligations to prevent money laundering and terrorist financing are to be met in full and are to be applied as a minimum standard;
- Positive management action will be exercised in order to minimise the risk of Sunstar being abused for the purpose of laundering of funds associated with criminal activity, or being used as a vehicle for terrorist financing;
- Sunstar will not continue established relationships with customers whose conduct gives rise to suspicion of involvement with illegal activities unless directed to do so by law enforcement. Sunstar will seek to terminate any customer relationship where the conduct gives the Company reasonable cause to believe or suspect involvement with illegal activities. Any such termination shall follow the reporting of suspicions to the Financial Intelligence Unit and dealt with accordingly in liaison with the relevant authorities.

Procedures are maintained to ensure the following:

- The identities of persons conducting business with Sunstar are properly identified and verified, and sufficient information gathered and recorded to permit Sunstar to 'know its customer' and predict the expected pattern of business;
- Potential new relationships that do not appear to be legitimate or where there is suspicion relating to criminal conduct on the part of the potential customer are referred to the MLRO before any relationship is entered into;
- Established relationships are regularly monitored to ensure they remain fit for the customer's profile, especially in respect of large or abnormal transactions;
- Records are retained to provide an audit trail and adequate evidence to the financial information unit or law enforcement for investigatory purposes;
- All suspicions are reported promptly in accordance with the internal procedures and, where applicable, reported to the Financial Intelligence Unit in accordance with the relevant procedures;
- That Sunstar has vigilant systems and processes implemented which are routinely monitored and tested for effectiveness to help combat money laundering and terrorist financing.

The following outlines an analysis of the AML risks faced by the Company. This shall be reviewed and updated on a regular basis, at least bi-annually:

	Risk Factor	Comment	Risk	Mitigation to lower risk	Residual Risk
Customers	Identifying Customers and obtaining KYC	Upon higher accumulated transactional volumes-reaching the threshed of EUR 1800, KYC shall be requested (CDD measures), as well as upon detection of any suspicious behavior such as, but not limited to, possible third-party usage, linkage to another existing account/s, ML suspicions, etc.	Medium		Low
	Staff knowledge of players?	Staff are expected to have a very good understanding of regular and HNWI players' activity.	Low	Training provided on a range of ML/TF and technology-based risks related to cryptocurrency gambling and the potential risks associated with the combination of both	
	Identifying of New Customers withdrawing to crypto	A manual review of newly registered Customers who request cryptocurrency withdrawal without having made prior deposits via cryptocurrency.	Low	Implementing EDD procedures for customers who request cryptocurrency	

				withdrawals without prior crypto deposits. This could include additional identity verification checks or proof of funds.	
	Alerts on cryptocurrency withdrawals	Company has automated alerts that activate upon a successful withdrawal when a cryptocurrency wallet is detected to have been used on a different account. Every first crypto withdrawal of an user is always manually reviewed and his/her betting account fully audited prior to processing the payout.	Low		
	Closed Loop	Upon detecting that a customer is funding their account via cryptocurrency and withdrawing through a different payment method (or vice versa), a revision of the account activity will be initiated, including assessing potential money laundering (ML) risks, analyzing for 1:1 turnover, identifying low-risk gameplay patterns, and other suspicious behaviors.	Low		

Location of participants

A participant located in a jurisdiction which is not Financial Action Task Force (FATF) compliant, may generally be considered to represent a potential risk of ML/TF activity. However, it is management's considered opinion that an individual transacting with the Company in what may be considered a normal manner, but from such a territory, represents only a minimal enhanced risk of ML/TF.

Whilst the above factors are considered when determining the identification requirements at registration, Management considers that other factors, when combined with the above, create heightened risk of on-going ML/TF activity. These contributory factors include but are not limited to:

- Amount of funds being transacted
- Nature and frequency of transactions

In order to determine the participant risk, these factors will be considered on a case-by-case basis. IP cross-referencing can be conducted where there may be any doubt of a customer's ownership of a particular wallet or location.

At present the Company does not allow individual participants, both residents and visitors, to utilise any of the Company's products or services from jurisdictions outlined in its blocked jurisdiction resolution.

A monthly review is conducted by the compliance team across all registered participant jurisdictions. The review monitors both AML/CFT and commercial consideration. The monthly overview of the jurisdictions takes place in order to check that players have not been accepted from FATF closed or deficient jurisdictions. This review is monitored and reviewed by senior management, including the MLRO.

Amounts of funds being transacted

The Company is aware of the payment requirement threshold set in place by the GCB. If cumulative funds deposited or withdrawn are over the equivalent of the approximate value of Euros € 1,800 or a series of two or more related transactions, there is an enhanced risk of ML/TF activities and additional identity checks (CDD measures) are to be undertaken. The threshold is to be calculated on a daily basis taking into account all deposits and withdrawals since registration. If the requested information is not received within 30 days from the moment the threshold was reached, Company will terminate the relationship with the customer and report the transaction to the FIU if presumption of ML exists.

On-going monitoring for transactions

All transactions by all participants are recorded and can be monitored on a real time basis.

- Transaction monitoring will be undertaken on a real-time basis
- Conversion rates for value-based thresholds/alerts will be checked on a daily basis by the Operations team

It is recognised that a significant change to the normal operation of an account could be a sign of suspicious activity. A change may be:

- Unusually large deposits based on past deposit history
- Large deposits followed by large withdrawals combined with minimal betting transactions
- Multiple changes to address details

If, during the course of daily monitoring, it is noted that a player's profile has altered in a way that would alter their risk level an immediate review would be undertaken to ensure that all CDD criteria for the new risk level is met. Should any further documents or information be required the participant will be contacted with a request to provide such within a timely manner.

In addition, changes made to the participants identity and personal information will be reported on to the company's management. The evidence of identity previously provided by the participant will be reviewed and steps taken to renew and update that information in light of the reported changes to the participant's identity. In certain cases, this may mean that the account is suspended pending receipt of new identity and address verification. In the event that satisfactory confirmation of the information as to the identity of the participant or satisfactory verification of evidence of identity is not provided, then the account will be suspended, no further betting activity.

2. Cybersecurity Risk

The use of cryptocurrencies presents significant cybersecurity risks to the Company, as it may be targeted by cyber-attacks aimed at gaining unauthorized access to digital wallets, private keys, and other sensitive data. The decentralized and irreversible nature of cryptocurrency transactions makes such assets particularly attractive to cybercriminals. As such, the Company takes a proactive approach to safeguarding its digital assets through the following robust measures:

- Use secure cold wallets for long-term storage of cryptocurrencies

To mitigate the risk of wallet hacking and unauthorized access to private keys, the Company implements the following storage strategies:

Cold Wallets:

- ❖ The majority of the Company's cryptocurrency holdings will be stored in cold wallets, which are kept offline and isolated from the internet. Cold storage ensures that digital assets remain secure and inaccessible to hackers, even in the event of a network breach.
- ❖ Since the hardware wallets store the private keys offline, they are not susceptible to malware that may be present on computer or smartphone. This reduces the risk of phishing attacks or keyloggers stealing private information. Hardware wallets give full control over Company's funds.
- ❖ The Company holds its private keys and have complete ownership of Company's crypto assets, without relying on a third party to manage the funds.
- ❖ Most hardware wallets come with backup and recovery options, such as a recovery seed phrase. This allows Company to recover the funds in case the hardware wallet is lost or damaged.

Hot Wallet Management:

For smaller operational needs (e.g., instant player withdrawals), the Company will maintain limited amounts of cryptocurrency in hot wallets. These hot wallets will be subject to strict internal controls, including daily limits and real-time monitoring to detect suspicious activity.

Private Key Management:

Cryptocurrency wallets are controlled by “Private Keys”. These keys can be used from any location and device connected to the internet to access wallet funds. Once a private key has been compromised or exposed beyond the owner’s desire, there can be no assurance that other malicious actors will not continue to access the wallet and related funds at any point in the future.

Private keys will be stored securely, with restricted access granted only to authorized personnel.

Inherent Risk	<i>Private Keys Exposed or Stolen from Holder</i> The private keys (sometimes known as seed phrases) for any cryptocurrency wallet will always have the ability to authorize transactions from the related wallet. Multiple attack vectors and risks exist that can lead to the compromising of these keys and thus expose wallets to catastrophic loss. Malware/spyware infected device can relay inputs (such as keys) to malicious actors. Keys that are documented (e.g. on paper) can be lost by the holder and found by others not intended to have access to wallets. Malicious software and websites can request and capture private keys then relay these to malicious actors (e.g. fake wallet software such as MetaMask). Multiple people having seen a single set of private keys makes it extremely difficult to know who the initiator of a transaction is without the initiator declaring their actions. Single point of failure. Unintended capture of the private keys to a wallet will forever make that wallet unsecure Single point of failure. A transaction sent in error cannot be retrieved
Controls and Mitigation	Hardware wallets: Adds an airgap layer of security as private keys remain mostly offline while not in use. Increases availability of signatories without exposing private keys to software Although the controls and mitigations above significantly reduce the probability of identified risks, materializing the impact of compromised keys (even of all keys in the quorum) would remain catastrophic due to the finality of cryptocurrency transactions post-execution.

- Employ robust encryption techniques, firewalls, and security protocols to protect online wallets and payment gateways

The Company employs cutting-edge encryption and network security measures to safeguard its online cryptocurrency wallets and payment gateways:

End-to-End Encryption:

All data transmitted between the Company's systems, wallets, and third-party payment processors will be protected using end-to-end encryption, ensuring that any intercepted data remains unreadable to unauthorized entities.

SSL/TLS Encryption:

The Company's websites and platforms will implement Secure Sockets Layer (SSL) or Transport Layer Security (TLS) protocols, ensuring secure communication between the Company's servers and the users. This prevents man-in-the-middle attacks and secures players' data during deposits, withdrawals, and gameplay.

Firewalls and Intrusion Detection Systems (IDS):

Advanced firewalls will be deployed to prevent unauthorized access to the Company's internal systems. Additionally, Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) will be utilized to monitor network traffic for unusual activity and stop potential attacks in real-time.

Zero Trust Architecture:

The Company will adopt a Zero Trust security model, where no device, user, or system is trusted by default. This includes implementing strict access controls, continuously verifying all connections, and granting access only to those who need it for legitimate business purposes.

3. Risk of Flagged Funds

Receiving flagged funds in a crypto wallet can be a serious issue, as it may involve regulatory, legal, and financial consequences.

Reasons for flagging:

Once the funds get flagged, the whole string is flagged, which increases the chance flagged funds to be received. In case the crypto funds get flagged, exchanges may refuse to accept the transfer, which will cause cash flow issues. While there is a possibility of recovering flagged funds, it often involves a complicated and lengthy process that includes legal consultation, compliance with regulatory procedures, and potentially legal proceedings. The recoverability of flagged funds in a cryptocurrency wallet depends

on several factors, including the reason for the flagging, jurisdictional laws, and the actions taken by the relevant authorities.

The funds can be flagged due to suspicious activities, regulatory compliance issues, or security concerns (mainly illegal activities related to terrorism or drugs):

- ❖ Illicit activities: If the funds are flagged due to connections with illegal activities (e.g., money laundering, terrorist financing), recovery is unlikely. Authorities might seize these funds, and Company may need to prove that it was not involved in the illicit activities.
- ❖ Sanctions: If the funds are flagged due to sanctions, they may be frozen, and Company will need to comply with the relevant legal procedures, which might involve extensive documentation and legal processes.
- ❖ Scams or Fraud: If Company receives the funds due to a scam or fraud, the recovery might involve legal proceedings where Company will have to prove the case.

Third-party providers check for flagged funds by utilizing various compliance and blockchain analysis tools to monitor and track cryptocurrency transactions, involving blockchain monitoring, address screening, transaction pattern analysis, regulatory databases, real time alerts.

4. Risk of losing the ledger / access to it

The hardware wallets come with backup and recovery options that include a 24-word recovery seed phrase. This seed phrase is essential for restoring access to the wallet in case it is lost, stolen, or damaged. The Company's recovery process relies on these 24 recovery words, which act as a master key to regenerate the private keys and regain control of the crypto assets.

To ensure security, the keys are securely stored by the company's CEO in a physical safe box. Only the CEO has access to this safe, adding an additional layer of protection against unauthorized access. This setup ensures that the company can recover its crypto assets in an emergency while minimizing the risk of unauthorized access to the funds. Proper safeguards are crucial, as losing or exposing the recovery phrases could lead to irretrievable loss of the Company's assets.

5. Cryptocurrency Conversion Risk

Company engages a third party provider (payment service providers, PSP) for executing crypto currency exchanges which can pose a higher risk of ML/TF due to limited transparency in relation to the origins of funds or technical difficulties in establishing clear data. Since the PSP's solution is a software-based solution, it is vulnerable to hacking, posing a risk that the the Company's funds could be stolen if the provider's security is compromised or even if the business knowledge is less than that of the more knowledgeable users who may attempt to leverage payment products of this type to commit criminal acts or obfuscate the profits of such acts.

Additionally, transactions processed through the PSPs may originate from customers involved in illegal activities. This could result in the wallets used by the Company being flagged due to suspicious activity,

increasing regulatory scrutiny and potentially affecting the Company's ability to access or transfer funds. Proper safeguards and monitoring are essential to mitigate these risks.

Risk mitigation:

Company's Payments team defines maximum allowed balances per market and per currency based on their internal procedure and based on a documentation describing their approach to control and monitor the maximum allowed balances.

Monitoring of the balances is a responsibility of the reconciliation manager who oversees the respective market. The reconciliation manager reports the balances daily (working days only). The funds need to be kept within the approved maximum allowed balances. If the available balances in the PSP exceed the maximum allowed balance, the difference have to be settled to the dedicated hardware wallet.

To spread the risk a back-up PSP shall be onboarded.

Payment monitoring

Where indirect or converted payments are received, systems will check the origins of the funds being converted and alert to any potential link or proximity to crime or higher risk sources. The Fraud Team will investigate such alerts further or establish more details related to them and request assistance from other teams such as the MLRO where necessary to undertake appropriate assessment prior to payment processing. All payments that receive an alert or higher risk warning will be held/frozen until assessments have been completed. Indirect risk cases may require the freezing of customer funds and further CDD to assist with the establishment of a balanced but accurate analysis.

6. Financial risks

- Volatility Management: Implement conversion of cryptocurrency funds into stable assets (like fiat currency or stablecoins) to reduce exposure to price volatility.
- Liquidity Risk: Maintain a liquidity buffer to ensure that customer withdrawals and winnings are promptly honored, regardless of market fluctuations.
- Reserves and Limits: Set minimum and maximum transaction limits for deposits and withdrawals in cryptocurrency to manage cash flow and prevent excessive exposure.

7. Unauthorized Transactions

There is a risk of unauthorized transactions and potentially fraudulent activity occurring when a cryptocurrency wallet address is used across multiple accounts. This may indicate account compromise, unauthorized access, or wallet-sharing behavior, all of which pose security threats to the company's assets and customer funds.

Risk mitigation:

To mitigate this risk, the Company has implemented an automated alert system that triggers notifications whenever unusual patterns, such as the reuse of a wallet across different accounts, are detected. This system enables real-time monitoring and rapid response, helping to prevent unauthorized withdrawals and ensuring the integrity of cryptocurrency transactions.

8. Procedural Risk

All transactions are final and cannot be reversed by the sender. Any error or intentionally malicious execution of transactions that remove value from cryptocurrency wallets is non-recoverable except by physically locating the private keys of any receiving wallets involved in transactions.

Risk	<i>Transactions sent in error or maliciously</i> Due to the finality and irreversible nature of cryptocurrency transactions, key risks exist around the sending of assets from any wallet. 1. Single point of failure. A transaction sent in error cannot be retrieved. 2. Malicious code can be delivered via smart contracts and/or traditional viruses or malware that can trigger transactions from cryptocurrency wallets. 3. Cryptographic wallet addresses can be created in a number of different formats that are made up of alphanumeric characters. Remembering all the different characters of a wallet address is difficult and exposes risks related to malicious attacks where characters are replaced or where errors such as including spaces before or after an address can cause unintended loss. 4. Due to the complexity of addresses and transaction hashes (transaction receipts), signatories of transactions may ignore important details or authorise transactions without appropriate scrutiny of details.
Controls & Mitigation	Secure process guidance to proposing and authorising transactions: By documenting a procedure that includes information on how to authenticate the initiator, the value and intended recipient of a transaction, the risk of inappropriately reviewed or maliciously created transactions is greatly reduced. This could include the initiator notifying signatories of the intended transaction securely prior to making a transaction, as well providing specific details to be verified during the process by the other signatories.

9. Product and Technical Risk

Risk	Software failure Cryptocurrency software is based on smart contracts which are often created in programming languages that are highly specialised. This exposes a number of risks related to failure of the software and thus exposure of assets/wallets managed by it. 1. Critical vulnerabilities have caused catastrophic loss of cryptocurrency assets in the past due to failure of software that was intended to secure them 2. Malicious actors are constantly targeting software due to the high value nature of that software as a target for theft 3. Understanding and auditing the code for cryptocurrency wallet software is a relatively emergent aspect of blockchain and cryptocurrency. Selection of appropriate auditing standards and auditors can be challenging
Controls & Mitigation	Strong product selection process: • Selecting products based on available audits, ease of verification of software, audits and track record for software can provide greater assurance related to the security of the software High level of knowledge and awareness of software development • Being highly knowledgeable on both the history of software and its development can provide greater assurance regarding the historical and current risks posed to it Distribution of assets held by software • By allocating assets to multiple types of software, the risk of failure by one software type limits the total losses.

10. Licensing

Given the complex regulatory landscape for online gambling and cryptocurrency, the Company is committed to maintaining compliance with licensing requirements to operate legally and responsibly in each jurisdiction.

Licensing Procedures:

Obtaining and Maintaining Licenses

- The Company ensures that valid gambling licenses are obtained and maintained for the jurisdictions where it operates. Special attention is given to regions with specific requirements regarding cryptocurrency use, and any requirements are strictly followed.
- All licensing applications, renewals, and supporting documentation are managed proactively to ensure they are filed well ahead of renewal deadlines to avoid disruptions.

- The legal and compliance team oversees the accuracy and completeness of all licensing processes.

Adapting to Cryptocurrency Regulations

- Jurisdictions may impose specific rules on cryptocurrency transactions, such as KYC data requirements or reporting high-value transactions. The Company complies with these requirements as part of its licensing obligations.
- In jurisdictions with restrictions on cryptocurrency or where cryptocurrency gambling is not permitted, the Company will block or restrict services as needed to stay compliant.

Expansion into New Markets

- Before entering new markets, the Company performs thorough regulatory assessments to identify and meet licensing requirements, especially for any cryptocurrency-related provisions.
- As part of the expansion planning, the legal and compliance team consults with local legal experts and regulatory authorities to ensure full compliance from the outset.

Roles and Responsibilities

1. Management's responsibilities

Management is responsible for:

- The day-to-day compliance with AML and CFT obligations within the areas of Sunstar for which they are responsible;
- Ensuring the MLRO is provided with prompt advice of unusual / suspicious transactions and other matters of significance;
- Providing the Compliance Officer and with the appropriate resources to fulfil the function effectively, including unfettered access to systems, reports and processes to aid investigation and review; and
- Ensuring the MLRO has complete autonomy in any SAR review process to avoid any conflict of interest.

2. MLRO's Responsibilities

The MLRO is responsible for:

- Developing necessary policies, procedures, training and education of staff. The MLRO will ensure that associated guidance notes and internal documents are updated as and when changes to AML or CFT legislation occurs or any new developments are deemed worthy of bringing to the attention of the staff;
- Developing and maintaining policy in line with any advice and guidance from law enforcement and the Financial Intelligence Unit;
- Representing Company to all external bodies and third parties in relation to AML and CFT or compliance;
- Ensuring that Company continues to comply with its obligations within the policy and related procedures;

- Undertaking reviews of any suspicious activity reports and determining whether they should be reported to the Financial Intelligence Unit;
- Maintaining a register of disclosures and register of ML/TF enquiries;
- Managing consent requests; and
- Ensuring records are retained in an appropriate format and for the relevant time period in accordance with the legislation and regulations.

3. Compliance Officer's Responsibilities

The Compliance Officer is responsible for:

- Developing necessary policies, procedures, training and education of staff.
- Developing and maintaining policy in line with evolving statutory and regulatory obligations.
- Establishing, recording, and maintaining appropriate procedures and controls for monitoring and testing compliance with AML/CFT legislation.
- Ensuring the Operator has robust and documented arrangements for managing the risks identified by the business risk assessment.

4. Payments, Reconciliation and Fraud teams

Employees in Payments and Reconciliation teams are responsible for:

- Overseeing the flow of cryptocurrency deposits and withdrawals.
- Ensuring proper reconciliation of cryptocurrency transactions (deposits and withdrawals) to avoid discrepancies or misallocations.
- Maintaining sufficient cryptocurrency reserves to handle customer withdrawals, while managing conversion rates to avoid losses due to market volatility.
- Establish maximum balance thresholds for each market and currency based on factors such as transaction volumes, market volatility, liquidity needs, and risk exposure. Regularly review and adjust these limits to reflect changing market conditions, regulatory requirements, and company strategies.
- Create comprehensive documentation outlining the methodology and criteria used to determine maximum balance limits, including detailed descriptions of the risk assessment processes, liquidity planning, and market-specific considerations that influence the setting of these limits.
- Implement a robust system to continuously monitor account balances, ensuring they do not exceed the predefined limits.
- Generate regular reports that track adherence to the maximum balance policy and highlight any anomalies or breaches of established thresholds.
- Define and document procedures for escalating any incidents where account balances exceed the allowed limits.
- Outline corrective actions, including fund transfers, conversion processes, or other necessary measures to bring balances back within acceptable levels.

Employees in Payments team are responsible for:

- Remaining alert to the possibility of money laundering or terrorist financing

- Reporting all suspicions or knowledge to the MLRO in accordance with the reporting of suspicious activity policy;
- Monitoring transaction patterns for any anomalies that could indicate fraudulent activities or abuse of the system (e.g., money laundering).

5. IT team

IT team shall be responsible for Implementing cybersecurity measures, including encryption, secure wallets, and transaction monitoring tools, conducts regular system security checks and updates.

Staff Education, Training and Development

Given the rapidly evolving nature of cryptocurrency technology and the sophisticated tactics used by fraudsters, it is essential that the relevant employees are continuously educated and trained. Regular training ensures that staff are up-to-date on the latest compliance requirements, fraud detection tools, and blockchain analysis techniques. It empowers them to respond swiftly and accurately to real-time alerts, investigate flagged funds effectively, and mitigate emerging risks. Moreover, ongoing development programs build a culture of vigilance and accountability, reducing human error and ensuring that the team remains prepared to handle increasingly complex crypto-related risks. Investing in staff education not only strengthens operational security but also enhances the company's ability to protect its customers and maintain regulatory compliance.

Emerging Threats in Cryptocurrency Risk Management

The rapid evolution of cryptocurrency introduces new risks such as ransomware payments, DeFi fraud schemes, and evolving tax regulations.

The company monitors these trends and implements proactive measures to address them effectively.

Crisis Management Procedures

In the event of incidents like a major hack, flagged funds, or loss of private keys, the company will:

- Activate the responsible teams and notify key stakeholders.
- Secure affected systems to prevent further compromise.
- Conduct a forensic investigation to identify root causes.
- Report incidents to regulatory authorities and take remedial actions

Version Control

Document Name	Crypto Risk Management Policy
Version	1.0
Date	04 November 2024

Classification	Confidential
-----------------------	--------------

-

Version	Description	Date	Initials
0.1	Initial Draft	04/11/2024	

-

-