

Policy for the Handling of Distributed Ledger Technology (DLT) Assets

IT Management Santora B.V.

VERSION HISTORY

Version Number	Version Date	Author	Summary of Changes
V1.0	27/03/2025	Armine Gasparyan	

Contents

Introduction.....	4
Purpose.....	4
Scope.....	4
Definitions	5
Asset Acceptance	6
Asset Management and Storage	6
Storage Requirements	6
Backup and Recovery	7
Recovery tests.....	7
Transaction Authorization	7
Transaction Verification.....	7
Access Control	8
Authorised Access	8
Role-based Access Control	8
Audit and Monitoring	8
Compliance and Legal Considerations	8
Regulatory Compliance	8
Audit and Reporting.....	8
Risk Management.....	9
Incident Response	9
Training and Awareness	9
Policy Review and Updates.....	9

Introduction

With the increasing adoption of Distributed Ledger Technology (DLT) such as blockchain, cryptocurrencies, and other decentralized platforms, IT Management Santora ('The Company') has implemented robust policies to securely manage and protect DLT assets used through its operation. These digital assets are susceptible to additional risks than traditional payments, including theft, fraud, and technical vulnerabilities hence to minimise such risk, the company has implemented various controls to be implemented during their storage, access, and transfer to ensure the integrity and security of both the assets and the organisation's operations.

This policy outlines the procedures for the management of DLT assets, including cryptocurrencies, and related technologies. It aims to safeguard the organisation from potential risks while maintaining compliance with relevant legal and regulatory requirements. This document is intended to provide a framework for all employees, contractors, and third parties who handle or interact with DLT assets, ensuring that these assets are treated with the highest level of security, accountability, and responsibility.

Purpose

The purpose of this policy is to establish guidelines for the secure handling, management, and operational use of Distributed Ledger Technology (DLT) assets, including digital tokens, cryptocurrencies, and other assets transacted or managed using blockchain or similar technologies. This policy aims to ensure that all DLT-related activities are conducted in compliance with applicable laws, regulations, and best practices to protect organisational and client assets from theft, fraud, and unauthorized access.

Scope

This policy applies to all employees, contractors, and third parties who have access to or are responsible for the management, transfer, or use of DLT assets in any form. This includes the administration, security, and handling of digital assets such as cryptocurrencies, utility tokens, security tokens as well as the management of private keys, wallets, and other related systems.

Definitions

DLT Assets: Includes digital assets or tokens stored on distributed ledger platforms (e.g., blockchain, DAG, etc.) that are used for transactions, investments, or as a form of payment.

Private Key: A cryptographic key that provides access to DLT assets and allows for signing transactions.

Public Key: A cryptographic key that is associated with a wallet and can be shared publicly to receive DLT assets.

Wallet: A software or hardware solution used to store, send, or receive DLT assets.

Cryptocurrency Exchange: A platform or service that facilitates the buying, selling, or exchanging of digital assets.

Cold Wallet: A wallet that is not connected to the internet and is used for long-term storage of DLT assets.

Hot Wallet: A wallet connected to the internet for quick access and transactions.

Asset Acceptance

When choosing a Distributed Ledger Technology (DLT) for digital assets to be accepted the following criteria are considered:

Scalability:

- Ability to handle high transaction volumes and grow without delays.

Security:

- Robust consensus mechanisms (e.g., Proof of Work, Proof of Stake).
- Strong data encryption to protect transaction data.
- Resistance to attacks, such as double-spending or 51% attacks.

Interoperability:

- Seamless integration with other blockchains or systems for cross-chain transactions.

Cost-effectiveness:

- Transaction fees and resource consumption should be reasonable.

Decentralization:

- No single entity should have too much control over the network.

Regulatory Compliance:

- Adherence to legal requirements for data protection and financial transactions.

The management will hold the final decision when approving new DLT to be accepted by the company as alternative method of payment.

Asset Management and Storage

Storage Requirements

DLT assets shall be stored securely using recognised and trusted digital wallets or custodial services. Private keys associated with the DLT assets must be stored in secure environments such as hardware wallets, cold storage, or multi-signature wallets. Access to private keys and wallets is restricted to the CTO and must be subject to robust authentication protocols in line with the Information Security Policy. Cold wallets should be used for the majority of assets. Hot wallets should only contain a small amount of assets necessary for day-to-day operations or transactions. Ratio should be kept at 90:10 subject to operations requirement.

Backup and Recovery

All private keys must be backed up securely and stored in multiple locations to prevent loss. Backup copies must be encrypted and only accessible to authorized personnel. A comprehensive recovery plan for DLT assets must be developed and tested regularly to ensure that in case of loss or corruption, assets can be restored.

Recovery tests

If a hardware wallet is lost or damaged, the recovery seed (typically a 12, 18, or 24-word phrase) must be used to restore the private keys onto a new device.

If private keys are stored in an encrypted file, the decryption password must be used to access the keys. The encrypted file should be decrypted using the appropriate software and password to regain access.

When storing private keys in cloud services (e.g., Google Drive, Dropbox), it is essential that the backup is encrypted and secured with a strong password to prevent unauthorized access.

Transaction Authorization

All transactions involving DLT assets, including transfers, exchanges, or withdrawals, must be authorized by at least one individual with the appropriate permissions.

High-value transactions or transactions to external addresses must require multi-signature approval or secondary verification from a designated manager or security team.

Transaction Verification

Before completing any transaction, the recipient address and transaction details must be verified to prevent sending assets to an incorrect or unauthorized destination.

Any transaction flagged as suspicious must be reviewed and approved by a designated compliance officer or security team.

Access Control

Authorised Access

Only authorized personnel are permitted to access DLT wallets and private keys. A list of authorized individuals must be maintained and reviewed periodically. All access to DLT wallets and systems must require multi-factor authentication (MFA) to enhance security.

Role-based Access Control

Different levels of access to DLT assets should be assigned based on the role and responsibility of the individual (e.g., administrators, users, auditors).

Privileged access, such as the ability to transfer or withdraw assets, is to key personnel and require additional authorization steps (e.g., multi-signature approval).

Audit and Monitoring

All transactions involving DLT assets must be logged and stored for audit purposes. Logs must include transaction details, timestamps, the identity of personnel authorizing transactions, and verification steps.

Continuous monitoring should be in place to detect any unauthorized access, unusual transaction patterns, or security breaches. Alerts should be configured to notify key personnel of any anomalies.

Compliance and Legal Considerations

Regulatory Compliance

All DLT asset-related activities must comply with applicable laws and regulations, including anti-money laundering (AML), know your customer (KYC), and taxation requirements.

Audit and Reporting

Periodic internal and external audits must be conducted to ensure compliance with this policy and identify any weaknesses in asset management practices.

Any discrepancies, fraudulent activities, or breaches of policy must be immediately reported to senior management and regulatory authorities if required.

Risk Management

All systems handling DLT assets, including wallets and exchanges, must be secured using the latest cybersecurity measures, such as encryption, secure protocols, and firewalls.

The use of cold storage and multi-signature wallets should be prioritized to reduce the risk of asset theft.

Incident Response

A detailed incident response plan must be developed for DLT assets, outlining steps to take in case of a security breach, asset loss, or system compromise.

Any incident or breach must be immediately reported to senior management and investigated to determine the cause and impact.

Training and Awareness

All employees handling DLT assets must receive regular training on security best practices, risk management, and compliance with this policy.

Training should also include recognition of common threats, such as phishing or social engineering attacks, and the proper response to such threats.

Ongoing awareness campaigns should be implemented to ensure that all individuals involved in handling DLT assets understand their responsibilities and the potential risks.

Policy Review and Updates

This policy should be reviewed at least annually or whenever there are significant changes in regulatory requirements, security practices, or the technology used for managing DLT assets.

Updates to this policy must be approved by senior management and communicated to all relevant stakeholders.

This policy is designed to ensure the secure and responsible handling of DLT assets, minimizing the risk of loss, theft, and regulatory non-compliance. By adhering to the guidelines set forth, the organisation can ensure the protection of digital assets while maintaining trust and operational integrity in all DLT-related activities.