May Payment SP. Z O.O. SEGREGATION OF CLIENTS' ASSETS POLICY AND PROCEDURES

Policy Name	Segregation of Clients' Assets Policy and Procedures	Version	2.0.
Drafted by	Internal legal and compliance team, strictly confidential and this information can be provided by the official request by the third party (Regulator, External Provider and/or Client)	Approved by Board on: 01.01.2026	
Responsible person	Internal legal and compliance team, strictly confidential and this information can be provided by the official request by the third party (Regulator, External Provider and/or Client)	Scheduled review date: 30.12.2026	

May Payment Sp. z o.o. (hereinafter referred to as "**May Payment**", "**our business**", "**Company**" "**we**", "**our**" or "**business**") Segregation of Clients' Assets Policy and Procedures (hereinafter referred to as "**Policy**") establishes the mandatory framework and procedures for the segregation and safeguarding of client assets held by us, a licensed Polish virtual asset custodian and exchange. The purpose is to ensure that all clients' funds and crypto-assets are held, managed, and recorded in accordance with applicable legal and regulatory standards, protecting clients' ownership rights and preventing misappropriation. The Policy ensures compliance with the EU Markets in Crypto-Assets Regulation (MiCA), Polish AML/CFT laws, ISO/IEC 27001 information-security standards, GDPR data protection, and relevant financial-sector best practices. It applies to all employees, officers, and third-party service providers of the Company, and supports transparency and accountability in custody operations.

1. REGULATORY FRAMEWORK AND LEGAL BASIS

This Policy is grounded in a comprehensive set of laws and regulations:

1. **Markets in Crypto-Assets Regulation (MiCA)** – Regulation (EU) 2023/1114 requires crypto-asset service providers (CASPs) to "make adequate arrangements to safeguard the ownership rights of clients" and to separate client crypto-assets from the firm's own. MiCA also mandates that client fiat funds (including stablecoins not qualifying as e-money) be placed in segregated accounts at credit institutions or central banks by the end of the next business day, and that those accounts be clearly distinguishable from the CASP's proprietary accounts. Therefore, MiCA explicitly governs custody services, requiring client custody agreements, internal custody policies, transaction registers, client statements, and legal/operational segregation of client assets. Losses of client crypto-assets due to the CASP's negligence are the sole responsibility of the CASP under MiCA.
2. **Polish AML/CFT Laws** – Under the Act of 1 March 2018 on Counteracting Money Laundering and Terrorist Financing (the "AML Act"), virtual currency service providers must establish AML/KYC policies, appoint a qualified AML officer and MLRO, conduct customer due diligence and ongoing monitoring, and apply a risk-based approach to transactions. Firms must also implement procedures for secure data storage and maintain records of transactions, and report suspicious activity to the General Inspector of Financial Information. These AML obligations reinforce the need to accurately track and retain custody records and customer identity information.
3. **ISO/IEC 27001:2022 (Information Security Management)** – The Company's information security management system (ISMS) conforms to ISO 27001, providing a risk-based framework to protect all sensitive information assets, including cryptographic keys and customer data. ISO 27001 prescribes policies and controls (e.g. encryption, access management, asset inventory, incident response) to ensure confidentiality, integrity, and availability of data. These controls apply in particular to the custody and transfer of virtual assets, requiring secure key management, backup, and logging in accordance with best practices.
4. **GDPR (Regulation (EU) 2016/679)** – As a data controller and processor of personal data in Poland, the Company implements "appropriate technical and organisational measures" to secure personal data, including encryption, access controls, and testing of security measures. The handling of clients' personal and transactional data should comply with GDPR principles (lawfulness, purpose limitation, data minimization, security, and confidentiality), including performing Data Protection Impact Assessments for high-risk processes.
5. **EU Financial Sector Best Practices** – Industry guidance (e.g. AFME principles) emphasizes full segregation of client assets and accounts. The Company's approach aligns with established frameworks in securities and payments sectors for segregating internal and external accounts, multi-signature custody solutions, and periodic audits to protect client assets.

2. DEFINITIONS:

1. **Crypto-Asset:** A "digital representation of value or rights that may be transferred and stored electronically, using distributed ledger or similar technology" (MiCA Art.2). This includes cryptocurrencies (e.g. Bitcoin, Ethereum), tokens (ERC-20, NFT, etc.), and stablecoins not qualifying as e-money tokens.
2. **Client Assets:** Any fiat currency, token, or cryptocurrency that belongs to the Company's clients (customers) and is held or controlled by the Company on their behalf. Client assets do not include the Company's own proprietary funds or investment holdings.
3. **Hot Wallet:** A cryptocurrency wallet that is connected to the internet and used for active, frequent transactions (e.g. facilitating exchanges or withdrawals). Hot wallets carry higher operational risk due to online exposure.
4. **Cold Wallet:** A wallet that is kept offline (e.g. hardware device, paper wallet, or air-gapped computer). Cold wallets are used to store the bulk of client assets securely, with multiple key-holders required for access.
5. **Multisignature (Multisig):** A cryptographic control where multiple private keys are required to authorize a transaction. The Company uses multisig configurations for high-value or cold-storage wallets to distribute trust and prevent single points of failure.
6. **Custody:** The safekeeping of crypto-assets or fiat funds, including the holding of private keys, maintenance of accounts, and execution of transactions on behalf of clients. Custody may be provided internally or via third-party custodians under agreement.
7. **Proprietary Funds:** Funds or crypto-assets owned by the Company itself, used for operational purposes (e.g. liquidity, treasury), and kept completely separate from client assets at all times.
8. **Segregation:** The practice of keeping client assets separate from proprietary assets both in records and actual custody, to protect client ownership rights and prevent commingling. Segregation is both legal (client assets are not part of the Company's estate) and operational (client assets are held in distinct wallets/accounts).
9. **Third-Party Custodian:** An external service provider contracted to hold or service client funds. Use of third-party custodians requires due diligence, contractual safeguards, and continued oversight by the Company.

3. ROLES AND RESPONSIBILITIES:

1. **Board of Directors** – They oversee the firm-wide risk and compliance program, approves the Asset Segregation Policy, and ensures adequate resources are allocated for custodial security. Please see herein the Key Personnel of the Company:

Key Personnel

Mrs. Oksana Dranenko – CEO & President of the management board member
LinkedIn link – https://www.linkedin.com/in/oksana-dranenko-811942346/

Head of Legal and Compliance Department at Company

https://docs.google.com/document/d/1rnLZ1VOmJ2YSGB9K87qNS4mGKennLKmp/edit

Head of Technical Support Department
https://docs.google.com/document/d/1ig_1Rt5HLWby08dH30OH8qpFxFIYZeUyxJIkbDvZLZ8/edit?tab=t.0

Anti-Money Laundering Officer and MLRO (AML reporting and risk compliance).

Mrs. Oksana Dranenko – President of the management board

Mrs. Oksana Dranenko is a highly experienced professional who possesses good knowledge and skills in business formation, business growth and development, strategy making and implementation, sales, business analytical skills and product development. Mrs. Oksana Dranenko is a great in line manager including performance management, motivation of staff, team building and delivering objectives within agreed timescales.

The professional experience of Mrs. Oksana Dranenko includes leading business operations of May Payment sp z.o.o for several month. Mrs. Oksana Dranenko has been a shareholder and managing director of several businesses in finance, MSB and other related areas as well in several jurisdictions.

Mrs. Oksana Dranenko has been leading May Payment sp z.o.o as the Shareholder and Director since September 2025 as a director, the director's main responsibilities consist of:

- developing and ensuring the execution of company's business plans;
- designing business development strategy;
- analyzing problematic situations and occurrences and provide solutions to ensure company survival and growth;
- delegating responsibilities and supervising the work of executives;
- providing guidance and motivation to drive maximum performance;
- Identifying and establishing sales leads and following up with approaches to appropriate target clients.

2. **President of the management board and Chief Executive Officer (CEO)** – **Mrs. Oksana Dranenko** maintains overall responsibility for implementing, enforcing this Policy and ensures senior management and key personnel is apprised of compliance issues and risk incidents.
3. **Risk Committee** – Compliance Officer and Information Security Officer conduct periodic risk assessments of custody operations (including cyber, operational, market risks), advise on mitigation strategies and review major incidents and corrective actions.
4. **AML Officer/MLRO** ensures compliance with MiCA and Polish AML/CFT requirements, including KYC/AML procedures and reporting. This includes appointment of a qualified person responsible for all AML/CTF obligations as required by law. The AML Officer/MLRO oversees customer due diligence (CDD), transaction monitoring, and suspicious activity reports.
5. **Information Security Officer (ISO)** implements, maintains the ISO/IEC 27001 ISMS, overseeing technical and organizational security controls, is responsible for key management procedures, access control enforcement, encryption standards, and incident response for security breaches and ensures staff receive security training and that regular audits of the ISMS are conducted.
6. **Operations / Custody Team** – They manage day-to-day asset handling. This team controls hot-wallet infrastructure, transfers between wallets, and interactions with third-party custodians. They ensure that internal accounting matches the actual on-chain or bank balances for all client funds. Only authorized personnel (with appropriate approval and multi-person controls) may execute transfers of client assets.
7. **Finance and Accounting** – They maintain the internal ledger of client accounts and corporate accounts, reconciles blockchain wallets and bank accounts with book entries, and produces periodic account statements for clients, and execute or verify client fund transfers in compliance with segregation rules.
8. **Internal Audit** – Either by Compliance Officer and Information Security Officer, independently reviews compliance with this Policy, tests controls (including reconciliation and segregation checks), and reports findings to the Board and management. Audits are conducted at least annually or as required by the management body.
9. **External Auditors / Regulators** – May audit or inspect custody practices. The Company will provide access to records and systems to authorized auditors or supervisory authorities to verify compliance with MiCA, AML/CFT, and data protection requirements.

10. **All Employees and Contractors** – Are responsible for following this Policy. Staff should not use client assets for any proprietary purpose, commingle funds, or bypass security controls. Any suspected violation or security incident should be reported immediately through the Company's incident reporting procedures.

4. PROCEDURES FOR ASSET SEGREGATION

The Company ensures that all client assets are legally, operationally, and technologically segregated from the Company's proprietary assets in accordance with applicable law (including EU MiCA Articles 75–76 and Polish AML/CFT laws) and industry best practices. Each client's virtual assets are held in a separate, identifiable wallet or account (or group of accounts) clearly designated as client-owned. At no time shall any client assets be commingled with the Company's own holdings or with those of other clients. The custody arrangement expressly precludes set-off: the Company will not use client assets to satisfy any of its own obligations and does not assume any proprietary claim on client funds. By virtue of fiduciary duty and statutory requirements, the client's crypto-assets remain the property of the client (held in trust or under fiduciary title) so that in the event of the Company's insolvency or bankruptcy, client assets are protected from claims by the Company's creditors.

The Company maintains a distinct register of positions (as required by MiCA that maps each client to the specific blockchain addresses or wallet identifiers holding their assets. This internal register is updated promptly upon client deposit, withdrawal, or transfer instruction. All transactions affecting client balances are recorded in real-time and evidenced by immutable blockchain transactions. The Company's custody policy minimizes loss of client assets by fraud or error, and a summary of this policy is provided to clients on request. At least every three months (and upon client request), the Company issues clients an electronic statement of position detailing each crypto-asset type, balance, value, and movements during the period, satisfying MiCA.

In compliance with MiCA and corresponding Polish law, client crypto-assets are legally segregated from the Company's estate. They are neither owned by the Company nor available to its creditors. The Company's internal accounting and legal framework treats client assets as trust property or subject to constructive trust. Operationally, client wallets are managed by a dedicated custody team with no authority to reassign those assets to any other purpose. The Company does not net client claims against any Company liability and does not re-hypothecate or pledge client crypto-assets. All access controls, keys, and user privileges are configured to enforce this segregation: employees authorized to handle client assets are prohibited by procedure and system design from transferring those assets into Company accounts except under a formal client order or contractual right.

The Company employs multiple advanced technical measures to enhance segregation and security. For example:

1. **Multi-Signature Key Management:** client wallets use multi-party cryptographic schemes (e.g. M-of-N multi-signature or threshold ECDSA) so that no single key or operator can unilaterally move assets. Private keys are held in Hardware Security Modules (HSMs) or secure hardware wallets, split across geographically-diverse locations or personnel.
2. **Sharding and Redundancy:** When generating wallet keys, the Company may use Shamir's Secret Sharing or similar techniques to break keys into shards, each stored on separate secure hardware. A quorum of key shares (e.g. 2 of 3) is required to reconstruct the key and initiate any transaction. This ensures that loss or compromise of any single component does not lose assets.

3. **Cold Storage (Vaulting):** The Company keeps the majority of client assets in cold "vault" wallets that are isolated from any network-accessible system. Vault access requires multiple independent authorizations (for example, two or more senior officers and an auditable process) and may involve air-gapped signing. Cold wallets are physically stored in secure facilities with environmental and intrusion protection. Only a minimal amount of assets needed for normal liquidity are held in hot wallets; hot wallets are limited to specific blockchains or tokens and are constantly replenished from the vault under controlled processes.
4. **Layer-2 and Cross-Chain Segregation:** For assets on layer-2 networks (such as Bitcoin Lightning channels or Ethereum rollups/sidechains) or cross-chain bridges, the Company treats each network similarly. Dedicated client addresses are used on each layer-2 solution, and any bridging of assets between chains is strictly controlled and logged. Layer-2 funds are never co-mingled with on-chain funds on the same private key, and network-specific segregation rules are enforced so that e.g. Lightning channel commitments correspond only to funds held in those channels on behalf of specific clients.
5. **Dedicated Custody Modules:** The Company may designate certain systems (software modules, subsystems, or hardware wallets) exclusively for client custody. For example, separate HSM devices or vault servers exist solely for client assets, with no unrelated software. Firewall and network segmentation ensure that custodial keys and signing infrastructure are isolated from trading or public-facing systems.

When the Company engages third-party custodians or sub-custodians (for example, for blockchains requiring institutional validators or for holding fiat in bank accounts), it imposes contractual obligations to maintain equivalent segregation. The Company uses only authorized CASPs per MiCA and requires any sub-custodian to hold client assets in separate, bankruptcy-remote accounts. The Company retains a right of audit and reviews SOC/ISO27001 reports from sub-custodians to verify their segregation and security controls. All agreements with sub-custodians explicitly forbid commingling of client assets with the sub-custodian's own funds. The Company shall notify clients (e.g. in the custody agreement or service terms) if any client assets are held via such third parties, and shall impose on them the same risk management and reconciliation standards that the Company applies internally.

5. OPERATIONAL CONTROLS

The Company's operational controls are designed to enforce the segregation policy and to secure client assets in compliance with ISO/IEC 27001:2022 standards and applicable laws (e.g. GDPR for data, AML/CFT for transactions). All systems and processes related to custody are subject to strict change management, access control, and monitoring. The following key controls are implemented:

1. **Access Management and Segregation of Duties:** Access to custodial systems (wallet controls, key management, and transaction systems) is tightly restricted. Role-based access control (RBAC) ensures that only authorized personnel can initiate or approve crypto-asset movements. At least two authorized individuals (e.g. a custodian and a compliance officer) should approve any large or critical transfer out of custody; no single person may both create and authorize a transaction ("four-eyes principle"). Privileged accounts (root, admin) are minimized and protected by multi-factor authentication. Regular reviews of user roles and permissions are conducted to prevent privilege creep. Responsibilities for custody operations, IT security, compliance, and audit are clearly separated.
2. **Cryptographic and System Security:** All sensitive operations (private key generation, signing, encryption) are performed in secure hardware (HSMs or certified wallets). Keys are encrypted at rest (e.g. using AES-256) and never exposed in plaintext on general-purpose servers. Communication between systems (internal APIs, node connections) uses encryption (TLS) and is monitored by intrusion-detection systems. Firewalls, network segmentation, and hardened operating systems

protect custodial infrastructure from external threats. Operating systems and software are patched promptly according to a formal patch management policy. Antivirus and malware detection tools are deployed on workstations and servers that handle any data related to client assets.

3. **Transaction Controls and Monitoring:** The Company employs automated limits and business rules to flag and prevent unauthorized transactions. For example, daily transfer limits per asset type, whitelisting of target addresses (with manual override), and geolocation/IP restrictions help prevent anomalous withdrawals. All transactions (incoming and outgoing) are logged in real time, and suspicious patterns (including, but not limited to, repeated small withdrawals, off-hour activity) trigger alerts to the security team. A separate AML/KYC control system flags large or high-risk transactions, and highly suspicious transactions are frozen and reported to the AML Officer/MLRO for potential filing of Suspicious Transaction Reports (STRs) with the Polish Financial Information Unit (GIIF).

4. **Data Protection and Privacy Controls:** Client personal data (identity documents, transaction history, etc.) is processed in accordance with GDPR and Polish data protection laws. Data is stored only as long as necessary, generally no longer than mandated by the AML Act (e.g. five years after end of business relationship) or other legal obligations. Access to personal data is restricted to personnel who require it for KYC/AML or service support purposes, and any transfer of personal data (including across borders) follows GDPR Chapter V safeguards. All systems storing personal data are secured with encryption at rest and in transit. Privacy Impact Assessments are conducted for significant changes to data processing systems. In compliance with GDPR, clients have the right to access their personal information and request corrections, subject to legal retention requirements.

5. **Segregated Data Storage and Backups:** The custody ledgers and transaction records are stored on systems that are logically and, when practicable, physically separate from the Company's trading and other business systems. Backups of wallet keys, transactional records, and client registers are taken regularly, encrypted, and stored in multiple secure locations. Backup cycles and retention periods meet both ISO 27001 and statutory requirements: for instance, transactional logs and audit trails are retained for a minimum of five (5) years (as required by the Polish AML Act and tax law) and then securely destroyed. Business-critical data (including cryptographic keys) is replicated to disaster-recovery sites with integrity checks to ensure recoverability.

6. **Change and Configuration Management:** All changes to custody systems (software updates, configuration changes) follow formal change management procedures. Proposed changes are reviewed and approved by the Security and IT teams, tested in a development environment, and logged in an audit trail. Emergency changes are documented and later reviewed. Configuration baselines for servers, wallets, and network devices are maintained and periodically audited to ensure no unauthorized modifications.

7. **Vendor and Outsourcing Controls:** Any third-party service providers (e.g. cloud hosting, key-management services, blockchain node providers) undergo due diligence before engagement. Contracts with vendors require compliance with ISO 27001 controls (or equivalent) and GDPR if they process personal data. Where crypto-assets are held by external custodians or banks, the Company includes terms requiring equivalent safeguards: separate accounts, audit rights, and immediate notification of incidents. The Company periodically reviews vendor performance and security (including, but not limited to, SOC2 reports or on-site assessments) to ensure continuous compliance.

8. **Training and Awareness:** Staff involved in custody and trading receive regular training on security policies, anti-fraud measures, and legal compliance (AML/KYC requirements, privacy obligations). The Company maintains a culture of security awareness, with periodic phishing tests and security bulletins to keep personnel alert to emerging threats (including, but not limited to, new attack vectors on crypto wallets).

6. RISK MANAGEMENT AND INCIDENT HANDLING

The Company maintains a comprehensive risk management framework to identify, assess, and mitigate risks to client assets. This framework aligns with ISO 27001:2022 (A.6, A.16–A.18) and MiCA

requirements, and is overseen by the Board of Directors and the Risk Committee. All material risks (cybersecurity, operational errors, market contagion, etc.) are documented in a Risk Register with assigned owners. The Company routinely performs risk assessments and stress tests (e.g. simulating large asset movements or cybersecurity breaches) to validate controls. Key risk mitigation measures include maintaining insurance (cyber and fidelity bonds) for crypto theft or loss, holding capital reserves, and requiring indemnity clauses in sub-custodian agreements.

The Company has an Incident Response Plan (IRP) that prescribes procedures for detecting, classifying, responding to, and recovering from security incidents or operational failures. The IRP categorizes incidents by severity (minor breach vs. major security incident) and defines roles and communication lines (IT, Legal, Compliance, PR, etc.). All employees should promptly report any suspected incident. The designated Response Team investigates incidents and documents timelines. Critical incidents trigger escalation to executive management and, if relevant, the Supervisory Authority (KNF) and/or FIU in compliance with EU incident-reporting rules (e.g. NIS2 Directive or GDPR breach notifications).

In the event of a suspected or confirmed loss, theft, or compromise of a cryptographic key or wallet, the Company executes a key-revocation and recovery procedure. The affected wallet is immediately frozen (by revoking signing capability). If a redundancy mechanism exists (e.g. other key shares or multi-sig partners), these are used to recover or reassign assets. All actions and communication are logged. If assets are confirmed lost or unrecoverable, the incident is treated as a reportable loss: the Company invokes its liability and insurance clauses to compensate clients up to the limits allowed under MiCA (capped at market value at loss time). The Company's legal team arranges restitution to affected clients promptly, either via insurance proceeds or, if necessary, using a crisis fund earmarked for this purpose. clients are notified immediately with a clear explanation of the event, steps taken, and remediation plan.

The Company complies with all statutory incident reporting requirements. This includes notifying the KNF or Polish Ministry of Finance of major operational disruptions, providing reports to the Financial Intelligence Unit (GIIF) for any suspicious activity related to asset movements, and informing the Data Protection Authority of any personal data breach. Incident reports include root-cause analysis and corrective actions. The Company cooperates fully with law enforcement and regulators (domestic and EU) in any investigation of asset theft or fraud, providing wallets' forensic data and transaction logs.

Consistent with MiCA, the Company is liable to clients for losses of assets or access keys caused by the Company's failures (capped at market value of the lost asset). The Company maintains a dedicated insurance policy covering theft, cyber-attacks, and employee malfeasance beyond the MiCA cap. If an incident qualifies as the Company's fault (including due to negligence or system compromise under our control), the Company will compensate clients from insurance or internal reserves. Under no circumstances will the Company use other clients' assets to cover losses; instead, it will reimburse each affected client individually. The Company's Custody Agreement (and any execution or sub-custody contracts) explicitly disclaims liability for market losses unrelated to security (e.g. crypto price volatility), but affirms coverage for unauthorized losses.

The Company also maintains a comprehensive Business Continuity Plan (aligned with ISO 27001/A.17 and ISO 22301). Critical systems (exchange matching engine, wallet servers, customer database) are backed up in real time to secondary data centers. Periodic drills (including, but not limited to, simulating data center failure or cyber-attack) are conducted to verify that the operations can resume within defined Recovery Time Objectives. An alternate staff roster ensures that essential custody functions can continue during emergencies (including, but not limited to, pandemic or regional outage).

7. MONITORING, REVIEW, AND AUDIT

Ongoing monitoring and periodic review ensure the effectiveness of segregation and security controls. The Compliance and Internal Audit departments conduct regular checks on custody operations, system logs, and reconciliation processes. Senior management receives quarterly reports on custody metrics (e.g. audit findings, security incidents, reconciliation status). The following measures are in place:

1. **Continuous Monitoring:** Automated tools monitor blockchain addresses for unauthorized changes, and compare on-chain balances against the Company's internal ledger of client positions at least daily. Discrepancies are investigated immediately. System health monitors (SIEM/IDS) watch for unusual login attempts or network activity on custodial systems. All access to custody systems (even read-only) triggers audit logging (user, time, action) with synchronized timestamps. Logs are retained in tamper-evident storage and protected against unauthorized deletion. Regular log reviews and audit log analysis are part of the security schedule.
2. **Reconciliation and Reporting:** The Company reconciles client balances with actual blockchain holdings on a frequent basis (daily or more often for high-volume assets). An independent reconciliation process (e.g. a team separate from the custodial operators) verifies that total client assets equal the sum of on-chain funds held in the designated wallets. Exceptions (such as unconfirmed blockchain deposits or pending withdrawals) are documented and cleared within a short time. Any systemic reconciliation discrepancies trigger escalation to senior management and the risk committee. Additionally, the company reconciles fiat liquidity (if holding client fiat in segregated bank accounts) with internal client fiat balances as part of its AML and PSP controls.
3. **Internal and External Audits:** An internal auditor (or compliance officer reporting to the Board) reviews the asset segregation and security controls at least annually. This audit covers policies, procedures, system configurations, and personnel compliance. Audits verify that segregation is upheld, that reconciliation is performed, and that any exceptions have been handled properly. The Company also engages external auditors (e.g. certified public accountants or cybersecurity firms) to conduct SOC/ISO audits of its custody environment. Audit findings are tracked to closure and corrective action plans are implemented promptly. The Company's policies, including this Segregation Policy, are reviewed at least annually and updated for changes in law (e.g. new MiCA guidance), technology, or business model.
4. **Regulatory Review and Compliance Checks:** The Company prepares and maintains documentation to demonstrate compliance with all applicable laws (MiCA, AML, GDPR, etc.). The Compliance department interfaces with the Polish Financial Supervision Authority (KNF) and the GIIF, providing periodic reports and undergoing on-site inspections or off-site reviews as required. Any regulatory feedback (such as an inspection finding) leads to immediate revision of procedures. The Company's official Custody Policy and agreements undergo review by legal counsel to ensure consistency with EU and Polish regulations.
5. **Metrics and Key Performance Indicators:** The Company tracks key metrics such as the number of successful reconciliations, frequency of security incidents, average response time to incidents, and audit issue closure rate. These KPIs are reported to the Board to ensure accountability. A culture of continuous improvement is maintained: lessons learned from incidents or audits feed into updates of the risk register and training programs.

8. REPORTING AND REVIEW

We conduct periodic internal audits of custody operations, security, and AML controls. Findings are reported to senior management with action plans. Key performance indicators (e.g. number of accounts opened, suspicious alerts, security incidents) are tracked monthly by the risk and compliance teams.

As a licensed CASP, we submit all required reports to the national regulator (e.g. client asset records, incident reports) and cooperate with supervisory reviews and inspections. Any major deficiencies or system outages are reported as per regulator deadlines.

This Policy is to be kept up to date to take into account changing circumstances. In this connection, this Policy provided herein will be updated periodically and at least annually on January 1 of each year to reflect any material change to our operations, infrastructure, business or business location(s).
Changes to systems (updates, infrastructure modifications) follow formal change control as per ISO 27002 to prevent inadvertent disruptions. The CMDB (configuration database) records disaster recovery dependencies. Release testing of software includes rollback procedures.

Major system changes or emerging threats (new attack vectors, regulatory changes) trigger plan updates. Internal audit or external review verifies compliance with standards (including, but not limited to, DORA requirements, EBA guidelines) and suggests improvements. We maintain an issues log and track corrective actions. Document control ensures only the latest approved procedures are in use.

This Policy and related policies are updated for new business activities or regulatory updates (including, but not limited to, MiCAR implementation acts, DORA technical standards, NIS2, etc.). Regular training and awareness programs keep staff prepared as per ISO 22301. By continually aligning with ISO 22301, ISO 27001 and industry best practices, the BCP remains robust and up-to-date.

We publish on our website a summary of this policy's key points (e.g. segregation, custody procedures, reporting). Fee structures and any material risks (including environmental impact of crypto-assets) are transparently disclosed. We maintain a clear complaints handling procedure and client service contacts.