SERVICE LEVEL AGREEMENT

MASCHAIN PLATFORM AND API SERVICES

Effective Date : 10th June 2026

1. **PREAMBLE**

1.1 This Service Level Agreement ("**SLA**") forms part of and is incorporated into the master services agreement, subscription agreement, or other principal written agreement entered into between **MASVERSE TECHNOLOGIES SDN BHD (Registration No. 202301043613 (1537529-X))** ("**MasChain**") and the customer identified therein ("**Customer**"), under which Customer is granted access to MasChain's blockchain platform and related services, together with any order forms, statements of work, schedules, or platform-specific terms entered into thereunder (collectively, the "**Master Terms**"). Capitalised terms used but not defined in this SLA have the meanings given to them in the Master Terms.

1.2 This SLA sets out the service availability commitments, incident response targets, service credit mechanism, support obligations, exclusions, limitations, and responsibility boundaries applicable to the Services.

1.3 In the event of any inconsistency or conflict between this SLA and the Master Terms in relation to service availability, service levels, support obligations, incident response, disaster recovery, business continuity, service credits, or other operational service commitments of a similar nature, this SLA shall prevail to the extent of such inconsistency, unless expressly stated otherwise in the Master Terms.

1.4 For the avoidance of doubt, this SLA does not relieve the Customer of any regulatory, statutory, supervisory, or compliance obligation applicable to the Customer. MasChain shall only be responsible for the obligations assumed by MasChain under this SLA and the Master Terms.

2. **DEFINITIONS AND INTERPRETATION**

2.1 In this SLA, unless the context otherwise requires, the following terms have the meanings set out below. Capitalised terms used but not defined in this SLA have the meanings given to them in the Master Terms.

"Authorised Contact"	:	means an individual designated by the Customer in writing (or via the Enterprise Portal) as authorised to report incidents, submit support requests, and receive communications under this SLA.
"Business Day"	:	means any day other than a Saturday, Sunday, or Malaysian federal public holiday.
"Business Hours"	:	has the meaning given in Clause 8.7.
"Critical (P1)", "High (P2)", "Medium (P3)", and "Low (P4)	:	have the meanings given in Clause 7.

"Customer"	:	has the meaning given in the Preamble. References to the Customer include each Authorised Contact acting on its behalf.
"Customer Confidential Information"	:	has the meaning given in Clause 12.1 (also referred to in this SLA as "**Customer Information**").
"Customer Personal Data"	:	means personal data (as defined under the PDPA) relating to the Customer's customers, employees, agents, or other natural persons, processed by MasChain in the course of providing the Services.
"Downtime"	:	has the meaning given in Clause 5.2(b).
"e-KYC"	:	means electronic Know-Your-Customer.
"Emergency Maintenance"	:	has the meaning given in Clause 6.2.
"Enterprise Portal"	:	means the online support, monitoring, and ticketing portal made available by MasChain to the Customer.
"Excluded Event"	:	has the meaning given in Clause 15.4.
"Maintenance Window"	:	means the recurring period of Sunday, 02:00 to 06:00 Malaysia Time ("**MYT**"), or such other period agreed in writing, during which MasChain may perform Scheduled Maintenance.
"MasChain"	:	means Masverse Technologies Sdn Bhd (Registration No. 202301043613 (1537529-X)).
"Master Terms"	:	has the meaning given in the Preamble.
"Measurement Period"	:	means each calendar month during the term of the Master Terms, used as the basis for calculating Monthly Uptime Percentage and any Service Credits payable under this SLA.
"Monthly Service Fee"	:	has the meaning given in Clause 9.2.
"Monthly Uptime Percentage"	:	means the percentage calculated in accordance with Clause 5.2(a).
"PDPA"	:	means the Personal Data Protection Act 2010 of Malaysia.
"RCA"	:	has the meaning given in Clause 8.5.
"Resolution"	:	shall be construed in accordance with Clauses 8.2 and 8.4.
"Response"	:	has the meaning given in Clause 8.3.
"Scheduled Maintenance"	:	means scheduled maintenance carried out by MasChain in accordance with Clause 6.1.

"Service Credits"	:	means the credits calculated and applied in accordance with Clause 9.
"Service Documentation"	:	means the technical specifications, API documentation, endpoint documentation, implementation guides, operational requirements, usage procedures, limitations and other service documentation made available or notified by MasChain to the Customer from time to time in respect of the Services.
"Service Tier"	:	means the Standard Tier applicable to the Customer pursuant to Clause 5.1.
"Services"	:	means the services described in Clauses 3.2 and 4, and any other service expressly stated in the applicable Order Form, Statement of Work, schedule or Service Documentation as being covered by this SLA.
"SLA"	:	means this Service Level Agreement.
"Standard Tier"	:	means the Standard service tier described in Clause 5.1.
"Sub-Processor"	:	means any third party engaged by MasChain to process Customer Personal Data on behalf of MasChain in connection with the Services, as contemplated in Clause 11.3.
"Transition Period"	:	has the meaning given in Clause 18.1.

2.2 Headings are inserted for convenience only and shall not affect the interpretation of this SLA. Unless otherwise stated, references to a "Clause" or "Schedule" are references to a Clause or schedule of this SLA. References to any statute, regulation, guideline, directive, notice, or other applicable law shall include any subsidiary legislation made under it, and any amendment, modification, replacement, or re-enactment of it from time to time. Words importing the singular shall include the plural and vice versa.

3. PURPOSE AND SCOPE

3.1 This SLA sets out the service availability commitments, incident response targets, support obligations, service credit mechanism, exclusions, limitations, and responsibility boundaries applicable to the Services provided by MasChain to the Customer. The purpose of this SLA is to define the minimum operational service standards applicable to MasChain's blockchain platform, application programming interfaces, enterprise portal, managed smart contract services, wallet services, token services, audit trail services, e-KYC services, and other related platform services made available by MasChain from time to time.

3.2 This SLA applies only to the Services and service components that are directly operated, managed, and controlled by MasChain. Unless expressly stated otherwise in the Master Terms, this SLA applies to the following service components:-

(a) the MasChain blockchain platform;

(b) MasChain application programming interfaces and API endpoints;

(c) the Enterprise Portal;

(d) managed smart contract deployment and interaction services;

(e) audit trail and on-chain verification services;

(f) wallet management services;

(g) token management services;

(h) NFT and certificate services;

(i) transaction query, explorer, and monitoring services;

(j) e-KYC services, where subscribed by the Customer;

(k) callback, webhook, and notification services provided by MasChain; and

(l) any other service expressly stated in the applicable order form, statement of work, schedule, or service documentation as being covered by this SLA.

3.3 This SLA does not apply to any unavailability, degradation, delay, failure, loss, or interruption arising from or relating to:-

(a) Customer systems, applications, databases, networks, devices, wallets, private keys, credentials, integrations, or internal infrastructure;

(b) third-party systems, service providers, identity service providers, telecommunications networks, internet service providers, cloud platforms, hosting providers, payment systems, or external APIs not directly controlled by MasChain;

(c) public blockchain networks, third-party blockchain networks, bridges, wallets, protocols, explorers, or smart contracts not operated or controlled by MasChain;

(d) Customer-side configuration errors, misuse, unauthorised access, failure to follow MasChain's technical documentation, or failure to implement required updates or security measures;

(e) Scheduled Maintenance, Emergency Maintenance, or other exclusions expressly stated in this SLA;

(f) force majeure events, cyberattacks, denial-of-service attacks, malware, regulatory intervention, or other events beyond MasChain's reasonable control; or

(g) legal, regulatory, compliance, commercial, financial, or business outcomes arising from the Customer's use of the Services.

3.4 MasChain is responsible only for the availability and performance of the Services under its direct operational control. The Customer remains responsible for its own systems, data, users, access controls, compliance obligations, business processes, customer onboarding decisions, transaction instructions, and use of outputs generated through the Services.

4. **SERVICES**

4.1 Subject to the applicable Master Terms, Order Form, Statement of Work, schedule, service documentation and any other written agreement between the Parties, this SLA applies to the Services described in this Clause 4.

4.2 MasChain may update, enhance, modify, suspend, replace or retire any Service, service feature, functionality, interface, API, endpoint, infrastructure component or related service documentation from time to time in accordance with the Master Terms, provided that such change shall not materially reduce the overall service commitments expressly agreed with the Customer, unless otherwise agreed in writing.

4.3 The Services covered by this SLA include the services set out in the table below, together with the applicable Service Documentation. The Services are more particularly described as follows:-

No.	Service	Service Description	Covered Capabilities
1.	Audit Trail Service	The Audit Trail Service provides Customers with a robust, tamper-resistant mechanism for recording, maintaining and verifying data provenance on the MasChain blockchain. Records submitted through the Audit Trail Service are cryptographically hashed and immutably stored on-chain, enabling a verifiable audit trail for data integrity, compliance, governance and operational audit purposes. The Audit Trail Service is intended for use cases where data authenticity, traceability and chain-of-custody records are important, including supply chain management, healthcare and other compliance-sensitive environments. The Audit Trail Service is intended for use cases where data authenticity, traceability and chain-of-custody records are important, including financial services, supply chain management, healthcare, regulated technology platforms and other compliance-sensitive environments.	(a) Smart Contract Management: Creation and retrieval of dedicated audit trail smart contracts per organization, supporting optional data encryption at rest. (b) Audit Record Creation: Submission of structured metadata records to the blockchain, with support for file attachments, category classification and tag assignment. Both application/json and multipart/form-data content types are supported. (c) Audit Record Retrieval: Querying of historical audit records from the database, filterable by category, tag or individual transaction ID. (d) On-Chain Transaction Verification: Direct retrieval of minted audit transactions from the blockchain, including block number, transaction hash, method and timestamp, with status filtering for success, pending and fail transactions and pagination support.

			(e) Record Amendment: Post-creation update of category and tag associations for an existing audit trail record. (f) Asynchronous Callback Notifications: Delivery of transaction confirmation or failure payloads to a Customer-specified callback URL upon finalization of each blockchain write operation. (g) Audit Category Management: Full lifecycle management of audit categories enabling Customers to logically classify records, including creation, update and deletion operations. (h) Audit Tag Management: Full lifecycle management of audit tags enabling granular labelling and filtering of records, including creation, update and deletion operations.
2.	Non-Fungible Token/ Certificate Service	The Non-Fungible Token Service, also referred to as the Certificate Service, enables Customers to deploy, issue and manage unique digital assets on the MasChain blockchain in accordance with the ERC-721 token standard. The service is intended for use cases requiring individual, non-interchangeable proof of ownership or authenticity, including digital certificates, academic credentials, professional licences, loyalty rewards and verifiable digital collectibles. Each NFT is minted together with associated metadata and stored using MasChain's managed storage infrastructure, producing a publicly accessible metadata URI and asset reference upon successful minting.	(a) Smart Contract Deployment: Creation of ERC-721-compliant NFT smart contracts with configurable parameters including token name, symbol, maximum supply or unlimited supply, owner wallet address and an optional contract logo image. (b) Smart Contract Retrieval: Listing and individual retrieval of deployed NFT smart contracts associated with the organization's API credentials, including contract address, token name, symbol and deployment transaction hash. (c) NFT Minting: Issuance of new NFTs to a designated recipient wallet address, supporting file attachments across four upload size tiers of up to 1 MB, 10 MB, 30 MB and 100 MB respectively,

			custom attributes, token name and description. (d) NFT Transfer: Peer-to-peer transfer of existing NFTs between wallet addresses, initiated by the contract owner. (e) NFT Record Retrieval: Querying of NFT records and transaction history, filterable by sender, recipient, contract address, transaction ID and status. (f) Contract Ownership Transfer: Irrevocable transfer of smart contract ownership to a designated wallet address, enabling organizational succession or delegation. (g) Asynchronous Callback Notifications: Delivery of minting and transfer confirmation or failure payloads to a Customer-specified callback URL.
3.	Custom Smart Contract Service	The Custom Smart Contract Service enables Customers to deploy, manage and interact with custom smart contracts on the MasChain blockchain without requiring the Customer to manage the underlying blockchain infrastructure directly. The service supports contract lifecycle management, including compilation, versioning, deployment and on-chain interaction through a structured project-based API framework. The Custom Smart Contract Service is intended for Customers requiring proprietary on-chain business logic, decentralised governance mechanisms, multi-party agreement execution or other applications	(a) Smart Contract Project Management: Organization of smart contracts into named projects with version tracking, enabling structured development workflows and lifecycle governance. Supports full CRUD operations on project records. (b) Smart Contract Version Management: Maintenance of compiled contract artifacts, including ABI and bytecode, across multiple versions within a project, enabling controlled promotion of contract versions to deployment. (c) Smart Contract Deployment: On-chain deployment of compiled contract artifacts via the API, with support for both custodial, organization-managed wallet execution and

		requiring programmable blockchain functionality beyond MasChain's managed token services.	non-custodial, Customer-signed wallet execution modes. Deployment gas consumption is tracked per contract instance. (d) Smart Contract Interaction — Read / Call: Invocation of view and pure smart contract functions without submitting an on-chain transaction, enabling data reads directly from contract state. (e) Smart Contract Interaction — Write / Execute: Submission of state-changing transactions to deployed contracts via either custodial wallet delegation or self-signed non-custodial transactions. Supports asynchronous callback delivery upon transaction receipt confirmation. (f) Token Transfer History: Retrieval of ERC-20 and custom token transfer logs associated with a specific deployed contract address. (g) Webhook Configuration: Management of webhook endpoints for receiving real-time smart contract event and transaction notifications. (h) Utility Endpoints: Supporting utilities including account nonce retrieval, token ABI lookup and wallet token balance queries. (i) Transaction and Account Queries: Retrieval of individual transaction details and receipts by hash, as well as account-level token transfer histories filtered by direction, whether to, from or bidirectional.
4.	e-KYC Service	The e-KYC Service provides Customers with a secure and fully digital solution for verifying customer identities in	(a) H5 Verification Link Generation: Creation of time-limited, tokenized verification URLs for delivery to end users. Supports

		real time. By using Optical Character Recognition, facial recognition and liveness detection technology, the service supports customer onboarding and assists Customers in meeting their know-your-customer compliance requirements, without requiring physical document submission or in-person verification. The service generates mobile-optimised H5 verification links to guide end users through the identity verification process. Upon completion, verification results may be retrieved through the applicable API for integration into the Customer's onboarding workflows. The service generates mobile-optimised H5 verification links to guide end users through the identity verification process. Upon completion, verification results may be retrieved through the applicable API for integration into the Customer's onboarding workflows.	two verification modes, namely full verification, comprising OCR, facial recognition and liveness detection, and document-only verification, comprising OCR only. Multiple national ID types are supported, including national ID cards and passports, across internationally recognized country codes in ISO-3166 alpha-3 format. (b) Verification Result Retrieval: Retrieval of the complete verification outcome for a given session token, including OCR extraction results, facial recognition outcomes, liveness detection results, overall success status, retry count and session expiry timestamp.
5.	Token Management Service	The Token Management Service provides Customers with a managed interface for the creation and lifecycle management of ERC-20 compliant fungible tokens on the MasChain blockchain. The service is intended for Customers seeking to issue digital currencies, utility tokens, loyalty points or other fungible digital assets requiring programmable issuance controls and transfer capabilities. Customers may maintain multiple independent ERC-20 token contracts, each with its own supply cap, decimal	(a) Smart Contract Creation: Deployment of ERC-20 token contracts via the Enterprise Portal, configurable with token name, symbol, maximum supply cap or unlimited supply by specifying 0, decimal precision, initial supply and designated owner wallet address. (b) Token Minting: Issuance of new tokens up to the configured maximum supply cap, credited to a specified recipient wallet address. (c) Token Burning: Permanent and irrevocable removal of tokens from a specified wallet balance, reducing total circulating supply.

		precision and ownership configuration. Tokens may support supply control through minting and burning, as well as pause and resume mechanisms to support operational control in the event of incidents.	(d) Token Transfer: Transfer of tokens between wallet addresses on behalf of the contract owner. (e) Token Pause: Suspension of all transfer activity for a token contract, restricting all inbound and outbound transactions until explicitly resumed. (f) Token Resume: Restoration of normal token transfer operations following a pause. (g) Balance Inquiry: Real-time retrieval of the token balance held by a specified wallet address for a given contract. (h) Contract Ownership Transfer: Delegation of token contract ownership to an alternative wallet address. (i) Transaction History: Retrieval of token transaction records filterable by wallet address, direction, whether to, from or bidirectional, and status, with pagination support. (j) Asynchronous Callback Notifications: Delivery of transaction confirmation or failure payloads, including full transaction receipt objects with log data, to a Customer-specified callback URL.
6.	Transaction Service	The Transaction Service provides Customers with visibility into on-chain activity across the MasChain blockchain. Through integration with MasChain's Explorer infrastructure, the service exposes transaction-level data, including decoded input parameters, event logs, token transfer records and gas usage metrics, enabling	(a) Transaction Detail Retrieval: Comprehensive retrieval of a transaction record by its hash, including sender and recipient address metadata, confirmation count, block number, gas consumption, transaction method, raw and decoded input data and token transfer sub-events.

		Customers to support monitoring, reconciliation and audit activities within their own applications. The service also allows Customers to configure how their transactions and associated entities are displayed on the public MasChain blockchain explorer, supporting brand consistency and transaction legibility for end users.	(b) Transaction Log Retrieval: Retrieval of decoded event logs emitted by a transaction, including event signatures, indexed topics, parameter types and values and associated block metadata. (c) Explorer Display Configuration: Management of how transactions, contract methods, raw inputs, decoded inputs, token transfers and event logs are presented on the MasChain public explorer, enabling Customers to control the visibility and granularity of on-chain data surfaces for their end users.
7.	Wallet Management Service	The Wallet Management Service provides Customers with a centralised and programmatic interface for managing the lifecycle of blockchain wallet accounts on the MasChain network. The service supports organization-owned custodial wallets and end-user wallets, enabling Customers to maintain separation of asset ownership and accountability within multi-stakeholder operational environments. In addition to wallet creation and retrieval, the service provides entity-level classification capabilities that allow Customers to group wallets by business unit, customer segment or operational category, supporting structured reporting and targeted transaction filtering.	(a) Wallet Provisioning: Creation of blockchain wallet accounts for both organizational use and end-user assignment, with automatic key management handled by MasChain's custodial infrastructure. End-user wallet creation supports identity metadata fields including name, email and national identification number. (b) Wallet Retrieval: Listing of all wallets associated with the organization's API credentials, filterable by wallet type, whether organization or end-user, with full detail retrieval by individual wallet address. (c) Wallet Lifecycle Management: Activation and deactivation of wallet accounts to control their eligibility for transaction execution, without permanent deletion. Wallet metadata, including display name and entity association, may be updated post-creation. (d) Transaction Nonce Inquiry: Retrieval of the current transaction nonce count for a

			given wallet address, supporting accurate transaction sequencing for non-custodial signing workflows. Supports block state queries, namely pending, latest, earliest, safe and finalized. (e) Wallet Category Management: Creation and management of organizational wallet classification categories, enabling structured grouping of wallets for reporting and operational segmentation. (f) Entity Management: Definition and management of organizational entities, being discrete business units or customer groups to which wallets and wallet categories may be associated, providing a hierarchical organizational model for asset management. (g) Entity Category Management: Classification of organizational entities into logical groupings, providing an additional layer of structural segmentation for enterprise-scale deployments.

4.4 The technical specifications, APIs, endpoints, supported functions, operational requirements, limitations, dependencies, usage procedures and implementation requirements for each Service shall be set out in the applicable Service Documentation, as may be updated by MasChain from time to time in accordance with the Master Terms.

4.5 The Customer shall comply with the applicable Service Documentation when accessing or using the Services, including any authentication, API, configuration, data formatting, operational, integration or security requirements specified by MasChain.

4.6 Unless expressly stated otherwise in the applicable Order Form, Statement of Work, schedule or Service Documentation, this SLA applies only to the Services expressly subscribed for or purchased by the Customer, and not to any service, feature, module, API, endpoint or functionality which has not been made available to the Customer under the applicable commercial arrangement.

5. **SERVICE AVAILABILITY COMMITMENT**

5.1 MasChain shall use commercially reasonable efforts to make the production Services directly operated, managed, and controlled by MasChain available in accordance with the following Monthly Uptime Commitment:-

Service Tier	Monthly Uptime Commitment	Eligibility
Standard	99.90%	Default tier applicable to Customers, unless otherwise agreed in writing in the applicable Order Form, Statement of Work, schedule or Master Terms.

The Monthly Uptime Commitment applies only to production Services that are:-

(a) expressly subscribed for or purchased by the Customer;

(b) directly operated, managed, and controlled by MasChain; and

(c) made available for production use under the applicable commercial arrangement.

For the avoidance of doubt, the Monthly Uptime Commitment does not apply to sandbox environments, test environments, beta features, proof-of-concept deployments, free trials, preview features, or any service, feature, module, endpoint, or functionality that has not been expressly subscribed for or purchased by the Customer, unless otherwise agreed in writing. Availability shall be measured at the relevant MasChain service boundary for the affected production Service.

5.2 Measurement of Uptime

(a) The Monthly Uptime Percentage shall be calculated as follows:

$$\textbf{Monthly Uptime Percentage} = \frac{\text{(Total minutes in the calendar month} - \text{Downtime)}}{\text{Total minutes in the calendar month}} \times 100$$

(b) For the purposes of this SLA, "**Downtime**" means any period during which the MasChain API is unable to accept or process valid API requests at the MasChain service boundary, as confirmed by MasChain's monitoring systems and corroborated, where reasonably practicable, by independent synthetic monitoring.

(c) MasChain's monitoring systems shall be the primary reference source for SLA calculations. Where the Customer reasonably demonstrates material discrepancies between MasChain's records and the Customer's own monitoring evidence, the Parties shall in good faith reconcile the relevant records and adjust the calculation accordingly.

(d) Downtime shall exclude Scheduled Maintenance, Emergency Maintenance and Excluded Events, provided that such exclusions are applied in accordance with this SLA.

6. MAINTENANCE

6.1 Scheduled Maintenance

(a) MasChain may perform scheduled maintenance from time to time for the purpose of maintaining the reliability, security, compliance, performance or proper operation of the Services.

(b) Where Scheduled Maintenance is expected to cause material service interruption, MasChain shall use commercially reasonable efforts to provide the Customer with at least seven (7) calendar days' prior notice.

(c) Where Scheduled Maintenance is not expected to cause material service interruption, MasChain shall use commercially reasonable efforts to provide the Customer with reasonable prior notice.

(d) Scheduled Maintenance shall, where reasonably practicable, be conducted during the Maintenance Window or at such other time as MasChain may notify to the Customer.

(e) Scheduled Maintenance periods shall be excluded from uptime calculations and shall not constitute Downtime.

6.2 Emergency Maintenance

(a) MasChain may perform emergency maintenance where reasonably necessary to address security vulnerabilities, active threats, service instability, platform integrity issues, data integrity issues, urgent technical issues, or other circumstances requiring immediate remedial action.

(b) Where Emergency Maintenance is required and service interruption is expected, MasChain shall use commercially reasonable efforts to notify the Customer in advance, where practicable.

(c) Where prior notice is not practicable, MasChain shall notify the Customer as soon as reasonably possible after commencement of the Emergency Maintenance.

(d) Emergency Maintenance periods shall be excluded from uptime calculations and shall not constitute Downtime.

6.3 Disaster Recovery and Business Continuity

(a) MasChain shall maintain commercially reasonable disaster recovery and business continuity procedures designed to support the continuity, restoration, and resilience of the Services under MasChain's operational control.

(b) MasChain's disaster recovery and business continuity procedures may include backup procedures, restoration procedures, incident escalation procedures, infrastructure recovery processes, and periodic internal review or testing, as MasChain considers appropriate for the applicable Services.

(c) Unless otherwise expressly agreed in the applicable Order Form, Statement of Work, schedule, or Master Terms, any recovery time objective, recovery point objective, disaster recovery test frequency, business continuity test frequency, or similar recovery commitment is provided as an operational target only and shall not constitute a guaranteed service commitment.

(d) The disaster recovery and business continuity procedures described in this Clause 6.3 apply only to systems and components under MasChain's operational control. They do not apply to Customer-managed systems, Customer integrations, third-party infrastructure outside MasChain's control, blockchain confirmation delays, forks, consensus events, public blockchain networks, or permanent on-chain records already confirmed on the blockchain.

(e) The Customer acknowledges that blockchain records confirmed on-chain are designed to be immutable and permanently retained as part of the applicable blockchain architecture.

7. INCIDENT SEVERITY CLASSIFICATION

7.1 Incidents shall be classified according to the severity levels set out in the table below:-

Severity	Description
Critical ("**P1**")	A complete MasChain API outage, a security breach involving Customer data, or a critical incident affecting all or substantially all users. Core service functionality is unavailable and major Customer business functions are stopped.
High ("**P2**")	Significant service degradation, partial outage, or security issue affecting a material subset of users. Core features are impaired but remain partially functional.
Medium ("**P3**")	Minor service degradation or non-critical feature failure, where a workaround is available and the operational impact is limited.
Low ("**P4**")	Cosmetic issues, documentation errors, configuration queries, or general enquiries with no functional impact.

8. INCIDENT RESPONSE AND RESOLUTION TARGETS

8.1 MasChain shall provide support coverage as follows:-

(a) P1 incidents: 24 x 7 x 365;

(b) P2 incidents: Business Hours, with commercially reasonable efforts to respond outside Business Hours where the issue materially affects production use; and

(c) P3 and P4 incidents: Business Hours

8.2 The applicable target response times and target resolution times are set out below:-

Severity	Target Response Time	Target Resolution Time
P1	Within one (1) hour, 24 × 7	MasChain shall use continuous commercially reasonable efforts to restore the affected Service as soon as reasonably practicable.
P2	Within four (4) Business Hours	Within two (2) Business Days, or as soon as reasonably practicable depending on complexity.
P3	Within one (1) Business Day	Within five (5) Business Days, or in the next scheduled release where appropriate.
P4	Within two (2) Business Days	As determined by MasChain based on priority, release schedule, and operational impact.

8.3 For the purposes of this SLA, "**Response**" means acknowledgement of the incident by MasChain, confirmation that the incident has been logged, and an initial indication of the applicable severity classification or support category.

8.4 The target response times and target resolution times set out in Clause 8.2 are operational objectives provided on a commercially reasonable efforts basis. They do not constitute guaranteed resolution commitments and shall not give rise to Service Credits unless the relevant incident also results in Downtime causing MasChain to fail to meet the Monthly Uptime Commitment.

8.5 For P1 incidents, MasChain shall provide reasonable status updates during active incident management and may provide a workaround or interim mitigation where reasonably available. Where a P1 incident results in material Downtime, MasChain shall, upon the Customer's written request, provide a written incident summary within ten (10) Business Days after incident closure. The incident summary may include the nature of the incident, affected Service, duration, general cause, remedial steps taken, and any planned follow-up actions.

8.6 MasChain shall make available reasonable support channels for incident reporting, which may include email, support portal, ticketing system, or such other support channel notified by MasChain from time to time.

8.7 For the purposes of this SLA, "**Business Hours**" means 9:00 a.m. to 6:00 p.m. Malaysia Time ("**MYT**"), Monday to Friday, excluding Malaysian federal public holidays.

9. SERVICE CREDITS

9.1 Service Credit Eligibility

(a) If the Monthly Uptime Percentage falls below the Monthly Uptime Commitment for the Standard Tier, the Customer may be eligible for Service Credits calculated against the Monthly Service Fee in accordance with this Clause 9.

(b) For the Standard Tier, which has a Monthly Uptime Commitment of 99.90%, the applicable Service Credits are as follows:-

Monthly Uptime Percentage	Service Credit
Less than 99.90% and equal to or greater than 99.00%	5% of the Monthly Service Fee
Less than 99.00% and equal to or greater than 95.00%	10% of the Monthly Service Fee
Less than 95.00% and equal to or greater than 90.00%	15% of the Monthly Service Fee
Less than 90.00%	25% of the Monthly Service Fee

(c) The maximum aggregate Service Credit payable for any calendar month shall not exceed twenty-five percent (25%) of the Monthly Service Fee for the affected Services.

9.2 Monthly Service Fee

For the purposes of this SLA, "**Monthly Service Fee**" means the recurring subscription fee paid by the Customer for the affected production Services during the relevant calendar month. Where the Customer has paid an annual subscription fee in advance, the Monthly Service Fee shall be calculated as one-twelfth (1/12) of the applicable annual subscription fee for the affected production Services.

Unless otherwise expressly agreed in the applicable Order Form, Statement of Work, schedule, or Master Terms, the Monthly Service Fee shall exclude usage-based fees, overage charges, top-ups, professional services fees, implementation fees, integration fees, taxes, pass-through costs, third-party charges, and any fees for services not affected by the Downtime.

9.3 Service Credit Mechanics

(a) Service Credits shall be calculated on a monthly basis according to the applicable Monthly Uptime Percentage.

(b) Service Credits may be applied against subsequent invoices, future service fees, overage charges or additional services.

(c) Service Credits are not redeemable for cash, non-transferable and non-refundable.

(d) Service Credits shall not apply automatically. The Customer must submit a valid claim in accordance with Clause 9.6.

9.4 Sole Remedy

Subject to the carve-outs set out in Clause 13.3, Service Credits shall constitute the Customer's sole and exclusive financial remedy for any failure by MasChain to meet the Service Availability Commitment.

9.5 Repeated Service Availability Failure

(a) If the Monthly Uptime Percentage falls below 95.00% in any two (2) calendar months within a rolling six (6)-month period, the Customer may request a service review with MasChain.

(b) Following such service review, MasChain shall use commercially reasonable efforts to identify the general cause of the repeated service availability failure and any reasonable remedial actions.

(c) Unless otherwise expressly agreed in the Master Terms, repeated service availability failure shall not create an automatic right to terminate the Master Terms, except where such failure constitutes a material breach under the Master Terms and remains uncured in accordance with the applicable cure period.

9.6 Service Credit Claims

(a) To be eligible for Service Credits, the Customer must submit a written claim within thirty (30) calendar days after the end of the affected month and provide reasonable details of the alleged Downtime, including the affected time periods, affected Services, and relevant API endpoints.

(b) MasChain shall determine eligibility for Service Credits based on its internal monitoring and operational records.

(c) Where the Customer reasonably challenges MasChain's calculation based on its own monitoring evidence, the Parties shall review the matter in good faith.

(d) Any approved Service Credits shall be applied to a future invoice for the affected Services.

10. INFORMATION SECURITY

10.1 Security Programme

(a) MasChain shall maintain a commercially reasonable information security programme designed to protect the confidentiality, integrity, and availability of the Services and Customer data processed by MasChain.

(b) MasChain's security programme may include administrative, technical, and organisational safeguards appropriate to the nature of the Services, the type of data processed, and the risks associated with the Services.

(c) Upon the Customer's written request, and subject to confidentiality obligations, MasChain may make available reasonable security documentation or summaries relating to its security practices, where available and appropriate.

10.2 Security Controls

MasChain shall implement and maintain commercially reasonable security controls, which may include the following:-

Security Control	Requirement

Encryption in transit	MasChain shall use commercially reasonable encryption protocols for external interfaces, where applicable.
Encryption at rest	MasChain shall apply encryption or other appropriate safeguards for sensitive Customer data stored in MasChain-controlled systems, where applicable.
Access control	MasChain shall maintain access controls designed to restrict access to Customer data and production systems to authorised personnel only.
Identity and access management	MasChain shall apply role-based access control and the principle of least privilege for access to production systems, where reasonably practicable.
Vulnerability management	MasChain shall maintain reasonable vulnerability management and patching processes based on severity, risk, and operational impact.
Application security	MasChain shall apply reasonable secure development practices in the design, development, testing, and deployment of the Services.
Security testing	MasChain may conduct security testing, vulnerability assessments, or penetration testing from time to time as MasChain considers appropriate.

10.3 Personnel Security

MasChain personnel with access to Customer data shall be subject to appropriate confidentiality obligations and internal security requirements. MasChain may provide security awareness or data protection training to relevant personnel as part of its internal policies and procedures.

10.4 Security Incident Notification

(a) MasChain shall notify the Customer without undue delay after confirming a security incident that materially affects the confidentiality, integrity, or availability of Customer Personal Data or Customer Confidential Information processed by MasChain in connection with the Services.

(b) Where reasonably practicable, MasChain shall provide the Customer with information regarding:-

(i) the general nature of the security incident;

(ii) the affected Services or data categories, to the extent known;

(iii) the measures taken or proposed to be taken by MasChain; and

(iv) a contact point for further information.

(c) MasChain shall provide reasonable updates as further relevant information becomes available.

(d) Any notification or cooperation under this Clause 10.4 shall not be construed as an admission of fault or liability by MasChain.

11. DATA PROTECTION AND PRIVACY

11.1 Compliance with Data Protection Laws

(a) In processing Customer Personal Data, MasChain shall comply with the Personal Data Protection Act 2010 of Malaysia and other applicable data protection laws to the extent applicable to MasChain as a service provider.

(b) MasChain shall process Customer Personal Data for the purpose of providing, maintaining, supporting, securing, and improving the Services, and otherwise in accordance with the Master Terms.

(c) The Customer shall be responsible for ensuring that it has obtained all necessary rights, consents, notices, permissions, and lawful bases required for the collection, use, disclosure, transfer, and processing of Customer Personal Data submitted to or processed through the Services.

11.2 Data Hosting, Residency and Cross-Border Transfers

(a) Unless otherwise expressly agreed in the applicable Order Form, Statement of Work, Master Terms, or Service Documentation, Customer Personal Data may be hosted and processed in locations determined by MasChain or its service providers.

(b) The Customer acknowledges that the provision of the Services may involve the transfer, storage, or processing of Customer Personal Data outside Malaysia.

(c) Where the Customer requires specific data residency, data localisation, or cross-border transfer restrictions, such requirements must be expressly agreed in writing in the applicable Order Form, Statement of Work, or Master Terms.

11.3 Sub-Processors

(a) MasChain may engage affiliates, contractors, service providers, hosting providers, infrastructure providers, and other third parties to process Customer Personal Data or Customer Confidential Information to the extent necessary to provide, maintain, support, secure, or improve the Services.

(b) MasChain shall take reasonable steps to ensure that such third parties are subject to confidentiality, data protection, or security obligations appropriate to the nature of the services provided by them.

(c) Upon the Customer's written request, MasChain may provide reasonable information regarding its material sub-processors, subject to confidentiality and security limitations.

11.4 Data Subject Rights

MasChain shall provide reasonable assistance to the Customer in responding to requests from data subjects exercising rights under applicable data protection laws, taking into account the nature of the processing and the information available to MasChain. The Customer shall remain primarily responsible for handling and responding to data subject requests relating to Customer Personal Data.

11.5 Data Return and Deletion

(a) Upon expiry or termination of the Master Terms, MasChain shall, upon the Customer's written request, return or delete Customer Personal Data held in MasChain-controlled off-chain systems within a reasonable period, unless retention is required or permitted by applicable law, the Master Terms, or MasChain's backup, archival, audit, security, or legal retention policies.

(b) MasChain shall not be required to delete records that are immutably recorded on-chain or records that MasChain is required or permitted to retain by law.

(c) The Customer acknowledges that blockchain records confirmed on-chain may be immutable, publicly verifiable, and not capable of deletion or alteration by MasChain.

12. **CUSTOMER CONFIDENTIAL INFORMATION**

12.1 Confidentiality

MasChain shall treat Customer Confidential Information ("**Customer Information**") as confidential and shall not access, use, disclose or process such information except:-

(a) as necessary to provide, maintain, support, secure or improve the Services;

(b) in accordance with the Customer's written instructions;

(c) as permitted under this SLA, the Master Terms or applicable Service Documentation;

(d) to approved personnel, affiliates, contractors, service providers or sub-processors who require access for the purpose of providing the Services and who are subject to appropriate confidentiality obligations; or

(e) where required by applicable law, court order, regulator direction, governmental authority or legal process.

12.2 Protection of Customer Confidential Information

MasChain shall implement reasonable administrative, technical and organisational measures designed to protect Customer Confidential Information against unauthorised access, disclosure, alteration, loss or destruction.

12.3 Exclusions

Customer Confidential Information shall not include information that:-

(a) is or becomes publicly available other than through a breach of this SLA by MasChain;

(b) was lawfully known to MasChain before receiving it from the Customer;

(c) is lawfully received by MasChain from a third party without breach of confidentiality obligations; or

(d) is independently developed by MasChain without use of or reference to the Customer Confidential Information.

12.4 Survival

The obligations in this Clause 12 shall survive expiry or termination of this SLA and the Master Terms for so long as MasChain retains Customer Confidential Information.

13. **LIABILITY BOUNDARY**

13.1 Limitation of Liability

Subject to Clause 13.3 and the Master Terms, MasChain's total aggregate liability under this SLA in respect of any failure to meet the Service Availability Commitment shall be limited to the Service Credits provided under Clause 9.

13.2 Exclusion of Damages

Subject to Clause 13.3 and the Master Terms, MasChain shall not be liable under this SLA for any indirect, incidental, consequential, punitive, exemplary, or special damages, including loss of profits, loss of revenue, loss of business opportunities, loss of goodwill, reputational damage, business interruption, or loss or corruption of data.

13.3 Carve-Outs

Nothing in this SLA shall exclude or limit liability to the extent such liability cannot be excluded or limited under applicable law. Any additional exclusions from limitation of liability, liability caps, indemnities, or special liability arrangements shall be governed by the Master Terms.

13.4 Insurance

MasChain may maintain insurance coverage as it considers appropriate for its business, operations, and the Services. Where specific insurance coverage is required by the Customer, such requirement must be expressly agreed in writing in the applicable Order Form, Statement of Work, or Master Terms.

13.5 Interaction with Master Terms

(a) This Clause 13 shall be read together with the corresponding limitation and indemnity provisions of the Master Terms.

(b) In the event of any inconsistency, the provision more favourable to the Customer shall prevail to the extent of the inconsistency, unless the Master Terms expressly state otherwise.

14. CUSTOMER RESPONSIBILITIES

14.1 General Responsibility

The Customer is responsible for ensuring that its use of the Services is properly configured, compliant and aligned with MasChain's technical and operational requirements.

14.2 Integration and Technical Implementation

(a) The Customer is responsible for implementing and maintaining correct integration with the MasChain API, including proper configuration, authentication and request formatting.

(b) The Customer shall ensure that all API requests submitted are valid, complete and compliant with MasChain documentation, and shall implement appropriate error handling, retry logic and failover mechanisms within its systems.

(c) The Customer shall ensure the compatibility of its systems with MasChain's supported interfaces and protocols.

(d) MasChain shall not be responsible for issues caused by incorrect implementation, malformed requests or improper use of the API.

14.3 Systems, Connectivity and Infrastructure

The Customer is responsible for maintaining its own systems, networks and infrastructure necessary to access and use the Services, ensuring reliable connectivity and adequate system performance, and monitoring its own systems for issues that may impact service usage.

14.4 Security and Access Management

(a) The Customer is responsible for maintaining the confidentiality and security of API keys, credentials and access tokens, implementing appropriate internal security controls to prevent unauthorised access, and promptly notifying MasChain of any suspected security breach or compromise.

(b) The Customer acknowledges that any action performed using its credentials shall be deemed authorised by the Customer, save in cases of fraud or wilful misconduct attributable to MasChain personnel.

14.5 Data Accuracy, Retention and Usage

(a) The Customer is responsible for the accuracy, completeness and legality of all data submitted to the Services, for ensuring that its use of the Services complies with applicable laws and regulations, and for validating outputs and responses received from the Services where required for its own business processes.

(b) The Customer acknowledges and agrees that certain records submitted through the Services may be permanently recorded on the MasChain blockchain and, once confirmed on-chain, may not be modified, deleted, removed or erased due to the immutable nature of blockchain technology. Such records may include transaction hashes, smart contract states, token transfer records, audit trail entries, NFT minting records and blockchain verification metadata.

(c) MasChain may retain off-chain operational data, logs, metadata, indexes, uploaded files, webhook payloads and service records for operational, compliance, security, audit and disaster recovery purposes, including the following:

Data Category	Minimum Retention Period
API access logs	Minimum ninety (90) days
Webhook delivery logs	Minimum thirty (30) days
Transaction processing logs	Minimum one (1) year
Audit and compliance logs	Minimum seven (7) years, where applicable
Temporary processing files and retry queues	Operationally determined retention periods

(d) MasChain may archive historical operational records to cold storage or secondary systems. Retrieval of archived data may require additional processing time and may be subject to reasonable administrative or service fees.

(e) The Customer remains solely responsible for maintaining independent backups where required, complying with its own legal and regulatory retention obligations, and ensuring that no unlawful, restricted or non-compliant data is submitted where deletion may later be required.

(f) Where data or metadata has been permanently recorded onto the blockchain, MasChain does not guarantee the ability to delete, anonymise or remove such information from the distributed ledger. MasChain shall not be responsible for errors arising from incorrect, incomplete or non-compliant data provided by the Customer.

14.6 Compliance and Regulatory Obligations

The Customer is responsible for its own compliance with applicable regulatory, legal and internal governance requirements, and for performing any required due diligence, verification or validation when using the Services for regulated activities, including e-KYC, audit or compliance-related use cases. Use of the Services does not transfer the Customer's regulatory obligations to MasChain.

14.7 Acceptable Use and Conduct

(a) The Customer shall not misuse, overload or interfere with the operation of the Services, attempt to bypass security controls or access restrictions, or use the Services for unlawful, fraudulent or unauthorised activities.

(b) MasChain reserves the right to suspend or restrict access where such activities are detected, subject to reasonable prior notice to the Customer, save in cases of imminent risk to the platform.

14.8 API Rate Limiting and Traffic Management

(a) To preserve platform stability, security, fairness of usage and service availability, MasChain may implement API request rate limits, concurrency controls, throttling, traffic shaping and abuse prevention safeguards.

(b) Such controls may be applied on a per-customer, per-API key, per-IP, per-endpoint, per-service or platform-wide basis. Where applicable, MasChain may return standard rate-limit responses, including HTTP 429.

(c) The Customer is responsible for implementing appropriate retry logic, exponential backoff, request pacing, timeout handling and resilient integration practices.

(d) Repeated violations of reasonable usage thresholds, abusive behaviour, denial-of-service patterns, credential misuse or sustained operational disruption may result in temporary suspension, restriction or termination of API access. Any service degradation arising from such Customer behaviour may constitute an Excluded Event under Clause 15.

14.9 Cooperation and Incident Support

During incidents or investigations, the Customer shall provide reasonable cooperation and information requested by MasChain, respond to requests for clarification, logs or system information, and take reasonable steps to assist in identifying and resolving issues. The Customer acknowledges that any failure to provide such cooperation may impact MasChain's ability to meet the applicable response or resolution targets.

14.10 Effect on SLA

For the avoidance of doubt, any failure by the Customer to meet the responsibilities set out in this Clause 14 may impact service performance and availability. Any resulting issues may be treated as Excluded Events under Clause 15 and shall not be considered SLA breaches or qualify for Service Credits.

15. REGULATORY AND SECURITY OVERRIDES

15.1 General Principle of Responsibility

(a) MasChain shall be responsible for the operation, availability and performance of the Services, including the underlying blockchain network operated and controlled by MasChain, under normal operating conditions. SLA commitments shall apply to all service components within MasChain's direct operational control, subject to reasonable technical, operational and environmental limitations.

(b) MasChain shall operate and maintain the Services in accordance with applicable laws, regulatory requirements, and commercially reasonable, industry-aligned security practices, having regard to OWASP guidance, including the OWASP Top 10 where applicable, and equivalent international standards. For the avoidance of doubt, reference to such standards does not constitute certification, formal adoption or full compliance unless expressly stated.

15.2 Scope of Responsibility

MasChain's responsibility includes:-

(a) the operation of the MasChain platform and API services;

(b) the operation and maintenance of all blockchain nodes and network components under its control;

(c) the submission, processing and handling of valid API requests; and

(d) the implementation of commercially reasonable and industry-aligned security measures, including protection against distributed denial-of-service (DDoS) events.

15.3 Regulatory and Security Overrides

Notwithstanding any other provision of this SLA, MasChain may suspend, restrict, modify, throttle, delay, isolate or otherwise control access to, or operation of, the Services where MasChain reasonably determines that such action is necessary or appropriate for regulatory, legal, security, operational integrity or platform stability reasons. Such actions may include, without limitation, measures taken in connection with:-

(a) compliance with applicable laws, regulations, regulatory directions, enforcement requests, sanctions, court orders or governmental requirements;

(b) the prevention, investigation or mitigation of suspected unlawful, fraudulent, abusive, unauthorised or non-compliant activity;

(c) the preservation of the integrity, security or stability of the MasChain platform, API services, blockchain network or related infrastructure;

(d) temporary suspension of transaction processing, throttling, rate limiting, isolation of affected components or emergency operational measures to prevent systemic risk, cascading failures or material service disruption;

(e) security incidents, malicious attacks, distributed denial-of-service attacks, coordinated attacks, state-level attacks, zero-day exploits or other vulnerabilities, provided that MasChain has maintained appropriate security practices and the incident exceeds reasonable and proportionate mitigation capacity based on prevailing industry standards; and

(f) any Customer breach, misuse or abuse of the Services, including unlawful, restricted or non-compliant activities.

15.4 Excluded Events

SLA commitments shall not apply to any Downtime, degradation, performance issue, suspension, restriction, modification, throttling, delay, isolation or other control measure arising from or relating to any of the following events, circumstances or actions, each of which shall constitute an "**Excluded Event**":

(a) Customer Systems and Integration Issues: failures or issues caused by Customer systems, applications or infrastructure; incorrect API implementation, configuration or

integration; malformed, invalid or non-compliant API requests; or Customer-side network or connectivity failures;

(b) Third-Party Dependencies: failures or interruptions of third-party systems or services not under MasChain's direct control; third-party identity verification providers used in e-KYC; or external services or integrations configured or initiated by the Customer. Further details are set out in the Appendix;

(c) Infrastructure and Hosting Limitation: failures of underlying cloud infrastructure, hosting providers or data centres; large-scale internet outages or backbone disruptions; or hardware failures outside MasChain's direct administrative control despite reasonable safeguards;

(d) Network Integrity and Stability Measures: actions taken by MasChain to preserve the integrity, security or stability of the platform, including temporary suspension of transaction processing, throttling, rate limiting, isolation of affected components and emergency operational measures to prevent systemic risk or cascading failures;

(e) Security Incidents and Malicious Attacks: Downtime resulting from security incidents within reasonable and expected mitigation capabilities shall fall within MasChain's responsibility. However, SLA commitments shall not apply to incidents that: (i) exceed reasonable and proportionate mitigation capacity based on prevailing industry standards; (ii) involve large-scale, coordinated or state-level attacks; or (iii) exploit previously unknown vulnerabilities, including zero-day exploits, where MasChain has otherwise maintained appropriate security practices;

(f) Regulatory and Legal Compliance Actions: actions taken by MasChain in good faith where necessary to maintain compliance with applicable laws, regulations, regulatory directions, enforcement requests, sanctions, court orders or governmental requirements, including suspension, restriction or modification of the Services;

(g) Force Majeure: events beyond MasChain's reasonable control, including natural disasters, acts of God, acts of war, terrorism, civil unrest, national emergencies, widespread power failures and large-scale telecommunications or internet outages;

(h) Customer Misuse or Breach: suspension or restriction resulting from breach of the Master Terms, misuse or abuse of the Services, or unlawful, restricted or non-compliant activities by the Customer; and

(i) Blockchain Finality and Irreversibility: blockchain transactions processed through the Services may become permanent, immutable and irreversible once confirmed on-chain. MasChain does not guarantee the ability to reverse, cancel, amend, recover or invalidate any blockchain transaction, token transfer, smart contract execution, minting operation or on-chain record after network confirmation, unless such functionality is explicitly supported by the relevant smart contract design or service feature. API responses, transaction broadcasts, callback notifications and transaction receipt acknowledgements do not constitute guarantees of legal settlement finality, business completion or reversibility. The Customer shall be solely responsible for validating transaction parameters prior to submission, verifying recipient wallet addresses and instructions, and implementing appropriate approval, reconciliation and operational controls.

15.5 Effect of Regulatory and Security Overrides

For the avoidance of doubt, any Downtime, degradation, performance issue, suspension, restriction, modification, throttling, delay, isolation or other control measure arising from or relating to a Regulatory and Security Override or an Excluded Event shall not be included in Monthly Uptime Percentage calculations, shall not constitute a breach of this SLA, and shall not give rise to Service Credits. Notwithstanding the foregoing, where a Regulatory and Security Override or Excluded Event materially affects the Services, MasChain shall use reasonable efforts to mitigate the impact, communicate with the Customer and restore normal service as soon as reasonably practicable, having regard to the nature of the regulatory, legal, security, operational or Excluded Event issue. MasChain shall also provide the Customer with information reasonably necessary for the Customer's own regulatory notification obligations, where applicable and legally permissible.

16. REPORTING AND GOVERNANCE

16.1 Continuous Improvement

Upon the Customer's reasonable request, MasChain shall work in good faith with the Customer to identify and implement service improvements, including performance optimisation, security hardening initiatives and roadmap alignment relevant to the Customer's regulatory environment.

17. EXIT ASSISTANCE AND TRANSITION

17.1 Exit Assistance

Upon expiry or termination of the Master Terms for any reason, MasChain shall provide reasonable transition assistance to the Customer for a period of up to six (6) months, or such other period as may be agreed in writing by the parties, the "**Transition Period**". Such transition assistance may include:-

(a) continued provision of the Services during an agreed transition period;

(b) support in extracting Customer data held in off-chain systems in a structured, commonly used and machine-readable format;

(c) knowledge transfer to the Customer or its designated successor service provider;

(d) reasonable cooperation with any handover to a successor service provider; and

(e) provision of relevant integration documentation, technical materials and runbooks reasonably required for migration.

Unless otherwise agreed in writing, transition assistance may be subject to applicable fees.

18. GOVERNING LAW

18.1 Governing Law

This SLA shall be governed by, and construed in accordance with, the laws of Malaysia.

18.2 Jurisdiction

Subject to Clause 19.3 and the dispute resolution provisions of the Master Terms, the courts of Malaysia shall have exclusive jurisdiction over any dispute, controversy or claim arising out of or in connection with this SLA, including any question regarding its existence, validity, interpretation, performance, breach or termination. Where the Master Terms provide for arbitration or another dispute resolution mechanism, the dispute resolution provisions of the Master Terms shall prevail to the extent of any inconsistency.

18.3 Dispute Resolution

The parties shall first attempt to resolve any dispute in good faith through discussions between their senior representatives, escalated through the governance framework set out in Clause 17 of this SLA. If the dispute remains unresolved within thirty (30) Business Days from the date of the first written notice of dispute, either party may refer the matter to the courts of Malaysia, or to arbitration where applicable under the Master Terms.

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

APPENDIX A
THIRD PARTY DEPENDENCIES AND RESPONSIBILITY BOUNDARIES

1. **PURPOSE AND SCOPE**

(a) This Appendix identifies key categories of third-party dependencies used in connection with the Services and sets out the applicable responsibility boundaries between MasChain, the Customer, and relevant third-party providers.

(b) This Appendix applies together with Clause 15, including the provisions relating to SLA exclusions, service availability, responsibility boundaries, and Excluded Events.

(c) This Appendix is intended to clarify operational responsibility. It does not relieve MasChain of responsibility for matters within its reasonable control, including configuration, integration, monitoring, security settings, vendor coordination, escalation, and mitigation.

2. **CONTROL LEVELS**

For the purposes of this Appendix, the following control levels apply:-

(a) Direct Control

"**Direct Control**" means components operated and controlled directly by MasChain as part of its core service infrastructure. Where a dependency is under Direct Control, failures, delays, degradation, or disruptions shall remain within MasChain's responsibility unless caused by an Excluded Event under the Agreement.

(b) Shared Control

"**Shared Control**" means components where MasChain manages configuration, integration, orchestration, access controls, monitoring, vendor coordination, and service-level response, but where the underlying infrastructure, platform, or network is operated by a third-party provider. Where a dependency is under Shared Control, MasChain remains responsible for matters within its reasonable control, including its configuration, integration, monitoring, security settings, escalation, and mitigation obligations.

(c) Third-Party Control

"**Third-Party Control**" means components operated by an independent third-party provider, where MasChain does not directly control the underlying availability, performance, infrastructure, platform, network, or service operation of that provider. Where a dependency is under Third-Party Control, MasChain remains responsible for its integration with the provider, vendor coordination, monitoring, escalation, and reasonable mitigation efforts.

3. **DEPENDENCY MATRIX**

Dependency	Control Level	MasChain Responsibility	Third-Party Responsibility	SLA Treatment
Cloud Hosting	Shared Control	Configuration, deployment, monitoring, security settings, backups, access controls, and reasonable resilience design	Physical infrastructure, cloud platform availability, and provider-operated services	Excluded only to the extent caused by provider-side infrastructure or platform failure outside MasChain's reasonable control
SMS / Email Delivery	Third-Party Control	API integration, provider configuration, retry logic, monitoring, escalation, and error handling	Delivery networks, provider delivery systems, carrier networks, and email infrastructure	Excluded only to the extent caused by provider-side, carrier-side, or network-side delivery failure
OCR Provider	Third-Party Control	API integration, request handling, access controls, monitoring, fallback handling, and escalation	OCR engine availability, processing performance, and provider platform operation	Excluded only to the extent caused by provider-side OCR service failure
Face Recognition Provider	Third-Party Control	API integration, access controls, request orchestration, monitoring, fallback handling, and escalation	Recognition service availability, processing performance, and provider platform operation	Excluded only to the extent caused by provider-side face recognition service failure
Blockchain Validator Nodes	Direct Control	Node operation, monitoring, maintenance, security, availability, and performance	Not applicable, except external blockchain network conditions outside MasChain's control	Included in SLA unless caused by an external blockchain network event outside MasChain's reasonable control
Managed File & Asset Storage	Shared Control	Storage configuration, permissions, lifecycle rules, encryption settings,	Underlying storage platform availability and provider-	Excluded only to the extent caused by provider-side storage infrastructure failure

		monitoring, and retrieval integration	operated infrastructure	
DNS Providers	Shared Control	DNS records, routing configuration, domain administration, monitoring, escalation, and reasonable redundancy	DNS platform availability, registry-level issues, and global DNS propagation infrastructure	Excluded only to the extent caused by provider-side DNS failure, registry issues, or propagation failures outside MasChain's reasonable control
CDN Providers	Shared Control	CDN configuration, cache rules, origin settings, certificates, routing, monitoring, and escalation	CDN edge network availability and provider-operated content delivery infrastructure	Excluded only to the extent caused by provider-side CDN infrastructure failure
Payment Partners	Third-Party Control	Payment API integration, transaction request handling, reconciliation support, monitoring, escalation, and error handling	Payment authorisation, settlement, card networks, banking rails, fraud-screening systems, and payment partner platform availability	Excluded only to the extent caused by payment partner, card network, bank, or payment network failure

4. **SLA EXCLUSION STANDARD**

A failure, delay, degradation, or disruption involving a Shared Control or Third-Party Control dependency shall constitute an Excluded Event only to the extent that MasChain can reasonably demonstrate that:-

(a) the root cause originated outside MasChain's directly controlled systems;

(b) the incident was not caused by MasChain's misconfiguration, inadequate integration, security settings, access controls, monitoring, or operational processes;

(c) the incident was not materially contributed to or prolonged by MasChain's acts or omissions; and

(d) MasChain used reasonable efforts to monitor, escalate, mitigate, and coordinate with the relevant third-party provider.

A general involvement of a third-party dependency shall not, by itself, be sufficient to classify an incident as an Excluded Event.

5. **MASCHAIN RESPONSIBILITIES DESPITE THIRD PARTY DEPENDENCIES**

MasChain remains responsible for all matters within its reasonable control, including:-

(a) configuration of third-party integrations;

(b) secure management of credentials, keys, certificates, secrets, and access controls;

(c) monitoring of material dependencies;

(d) reasonable incident detection and escalation;

(e) implementation of retry logic, fallback handling, or graceful degradation where commercially reasonable;

(f) vendor coordination during incidents;

(g) maintaining reasonable records of incidents affecting the Services;

(h) applying available fixes, patches, configuration updates, or provider recommendations where applicable and commercially reasonable;

(i) avoiding foreseeable single points of failure where reasonable for the relevant Service; and

(j) communicating material service impacts to the Customer in accordance with this Appendix.

A third-party dependency shall not be treated as an Excluded Event to the extent the relevant failure, delay, degradation, or disruption was caused or materially worsened by MasChain's failure to perform the responsibilities set out above.

6. **SCOPE AND DURATION OF SLA EXCLUSION**

Any SLA exclusion arising from a third-party dependency shall apply only:-

(a) to the affected Service component;

(b) for the period during which the third-party dependency directly caused the relevant failure, delay, degradation, or disruption; and

(c) to the extent the impact could not reasonably have been prevented, mitigated, or reduced by MasChain.

Unaffected Service components shall remain subject to the applicable SLA.
Where an incident has multiple causes, only the portion of downtime or degradation reasonably attributable to the third-party provider or external dependency shall be excluded from SLA calculations.

7. **THIRD-PARTY INCIDENT NOTIFICATION**

Where MasChain confirms that a third-party provider incident materially affects the availability, performance, or functionality of the Services, MasChain shall use reasonable efforts to post a platform status notice through the MasChain Enterprise Portal within two (2) hours of confirming the third-party root cause. The notice should include, where reasonably available:-

(a) the affected Service component or functionality;

(b) the known or estimated impact on the Customer;

(c) the suspected or confirmed third-party dependency involved;

(d) mitigation steps being taken by MasChain;

(e) any workaround available to the Customer;

(f) any indicative resolution timeline made available by the third-party provider; and

(g) the time of the next expected update, where practicable.

MasChain shall issue a follow-up notice upon restoration of normal service or when the material impact has ended.

8. **EVIDENCE OF THIRD-PARTY CAUSE**

Where MasChain relies on a third-party dependency as the basis for excluding downtime, degradation, or failure from SLA calculations or Service Credit eligibility, MasChain shall maintain reasonable supporting records. Such records may include:

(a) provider status notices;

(b) provider incident reports or service advisories;

(c) monitoring data;

(d) incident tickets;

(e) internal incident timelines;

(f) logs showing the affected component or integration;

(g) escalation records; and

(h) mitigation steps taken by MasChain.

Upon the Customer's written request, MasChain shall provide a reasonable summary of the evidence supporting the claimed exclusion, subject to confidentiality, security, legal, and third-party contractual restrictions.

9. **PROVIDER SELECTION, MANAGEMENT AND CHANGES**

(a) MasChain retains responsibility for the selection, replacement, integration, and management of third-party providers used to support the Services.

(b) MasChain shall use commercially reasonable efforts to engage material providers that maintain appropriate operational, security, and availability standards, having regard to the nature of the relevant Service and dependency.

(c) Where applicable and commercially reasonable, MasChain will consider providers that maintain recognised security certifications or assurance reports, such as ISO 27001, SOC 2 Type II, or equivalent standards.

(d) MasChain may update, replace, or introduce third-party providers in the ordinary course of business, provided that such changes do not materially reduce the overall functionality, security, availability, performance, data protection standard, or regulatory compliance posture of the Services.

(e) MasChain shall provide advance notice where reasonably practicable of any planned provider change that is expected to materially affect the Customer's use of the Services, data processing arrangements, security posture, or service availability.

10. **CUSTOMER DEPENDENCIES AND CUSTOMER CAUSED ISSUES**

For clarity, MasChain shall not be responsible for failures, delays, degradation, or disruptions caused by systems, networks, configurations, credentials, devices, applications, service providers, or integrations controlled by the Customer or its users. Customer-side issues may include:

(a) Customer network or internet connectivity failures;

(b) Customer firewall, proxy, VPN, browser, endpoint, or device issues;

(c) Customer misconfiguration of APIs, webhooks, credentials, permissions, or access controls;

(d) Customer failure to maintain required integrations or software environments;

(e) Customer-provided third-party systems or data sources;

(f) unauthorised changes made by the Customer or its users; and

(g) failure by the Customer to follow reasonable technical requirements or implementation guidance provided by MasChain.

Such Customer-caused issues shall be excluded from SLA calculations and Service Credit eligibility to the extent they caused or contributed to the relevant failure, delay, degradation, or disruption.

11. **NON-EXHAUSTIVE DEPENDENCIES**

The dependencies listed in this Appendix are illustrative and non-exhaustive. MasChain may use additional third-party dependencies in connection with the Services. Any additional

dependency shall be assessed according to the same control-level, responsibility-boundary, evidence, and SLA-exclusion principles set out in this Appendix. The inclusion of a dependency in this Appendix does not automatically exclude all incidents involving that dependency from SLA calculations. The exclusion applies only where the requirements of this Appendix and Clause 15 are satisfied.

12. **ORDER OF PRECEDENCE**

In the event of any conflict between this Appendix and the main body of the Agreement, the main body of the Agreement shall prevail, unless the relevant provision expressly states that this Appendix is intended to override it. Nothing in this Appendix limits any liability that cannot lawfully be limited or excluded under applicable law.

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]