MASTER TERMS & CONDITIONS
VAULT SERVICES
Corporate Clients

Tesseract Investment Oy — Dedicated Client Vault (DCV) service

Table of Contents

Parties and recitals

These Master Terms & Conditions for Vault Services (the “Terms”) are entered into between Tesseract Investment Oy, a Finnish limited liability company with registered business ID 3476334-8, with its registered office Fredrikinkatu 47, 00100 Helsinki, Finland (“Tesseract”), and the Corporate Client whose particulars are recorded in Annex A (the “Client”), together referred to as “Party”.

WHEREAS, Tesseract is a crypto-asset service provider (“CASP”) under Regulation (EU) 2023/1114 (“MiCAR”) authorized by the Finnish Financial Supervisory Authority (FIN-FSA), covering custody and administration of crypto-assets, portfolio management of crypto-assets, and transfer services for crypto-assets;

WHEREAS, Tesseract has developed an on-chain discretionary crypto-asset strategy management product pursuant to which each client receives a dedicated, individually segregated vault deployed on smart-contract infrastructure (a “Dedicated Client Vault” or “DCV”), over which Tesseract holds the exclusive “owner” role to execute deployment actions on behalf of the client without at any stage taking beneficial ownership or proprietary possession of the client's crypto-assets;

WHEREAS, the Client wishes to appoint Tesseract as its (a) custodian and administrator of crypto-assets, (b) discretionary portfolio manager of crypto-assets, and (c) provider of transfer services for crypto-assets, in respect of the DCV, and Tesseract wishes to accept such appointment on these Terms;

NOW THEREFORE IT IS EXPRESSLY AGREED as follows. These Terms become binding on the Client's acceptance under Clause 31 and Tesseract's counter-acceptance; the Effective Date is the acceptance timestamp recorded in the Compliance App.

1. Definitions

1.1 In addition to terms defined in other provisions of these Terms and Conditions and the Annexes hereto, the following capitalized terms shall have the meanings ascribed to them below**:**

Airdrop	Is a distribution of new or additional tokens by reason of holding an existing crypto-asset.
Applicable Law	Means all laws, regulations, rules, orders, directives and guidance applicable to a Party or to the subject matter of these Terms, including MiCAR, the Finnish Consumer Protection Act (38/1978), the Finnish Bankruptcy Act (Konkurssilaki 120/2004), the GDPR, DORA, DAC8, and all applicable AML/CTF legislation.
Approved Protocols	Means the decentralized protocols and, where applicable, Tesseract's own proprietary strategy vaults into which Vault Assets may be deployed. Tesseract strategy vaults themselves deploy exclusively into whitelisted DeFi protocols.
Authorized Person	Means any individual authorized by the Client to act on its behalf, including by signing instructions through the Compliance App or the Vault Interface;
Client’s Custodian	Means any third-party custodian, wallet provider or other custody infrastructure provider designated by the Client to hold or control, on the Client’s behalf, the relevant wallet infrastructure, private cryptographic keys, key shards or other means of access used in connection with the DCV, the Vault Interface, any deposit into the DCV, any redemption from the DCV, or any related transfer or settlement flow.
Compliance App	Means the digital front-end at compliance.tesseract.fi through which the Client completes onboarding, KYC, KYB, AML and Travel Rule formalities, originates instructions and accesses information, including the SumSub identity integration.
Corporate Client	Means a Client that is a legal person (body corporate, partnership, foundation, association, trust or other non-natural-person entity), classified as such by Tesseract under the Suitability Policy.cc

DCV / Vault	Means the dedicated, individually segregated smart-contract vault established for the Client on the Ethereum mainnet, deployed as an ERC-4626 vault-token structure via the EIP-1167 minimal proxy pattern on IPOR Fusion infrastructure.
Deployment Actions	Means all actions taken by Tesseract on behalf of the Client within the DCV, including deposits to Approved Protocols, withdrawals, rebalancing and yield management, in accordance with the Investment Mandate.
Guardian Pause	Means the automated or manual mechanism that freezes Deployment Actions within the DCV to protect Vault Assets during identified risk conditions, technical anomalies, smart-contract exploits, oracle failures or material market disruptions (clause 6.2).
Hard Fork	Means a permanent divergence in a blockchain that may result in a new crypto-asset.
Investment Mandate	Means the investment mandate set out in Annex D, setting the parameters, guidelines, restrictions and risk limits governing Tesseract's discretionary management of Vault Assets.
Strategy	Means a named RCC-approved investment strategy operated through a Vault, drawn from the catalogue in Annex F (USDC Conservative; USDC Advanced; wBTC Advanced; wETH Advanced).
Product Information Summary	Means the per-Strategy summary document with the product overview, strategy, risk profile, indicative target return, costs and fees, liquidity, investor profile and key risks provided to the Client as pre-contractual disclosure for each available Strategy.
Super Admin / Owner Role	Means the exclusive administrative and control role held by Tesseract within the smart-contract architecture of each DCV, conferring the operational authority necessary to administer the Vault, effect Deployment Actions and otherwise control the DCV for the purposes contemplated by these Terms, without conferring beneficial ownership or proprietary entitlement to the Vault Assets.
Travel Rule	Means the originator and beneficiary information requirements applicable to crypto-asset transfers under Regulation (EU) 2023/1113 (recast Transfer of Funds Regulation) and its delegated/implementing acts.
Vault Assets	Means the crypto-assets deployed by the Client to the Decentralized Credit Vault (DCV) and managed therethrough, being as of the date of these Terms and Conditions the following Supported Assets: USDC, wETH and wBTC.
Vault Tokens	Means the non-transferable ERC-4626 tokens minted to the Client on deployment of Vault Assets, representing the Client's proportional claim on the assets in the DCV; they confer on-chain provable ownership and contractual rights evidencing a custody relationship supporting a claim for separation of assets under Chapter 5, Section 6 of the Finnish Bankruptcy Act.
Whitelisted Address	Means an address registered on the on-chain Whitelisting Contract referenced in Annex A.
Wind-Down Plan	Means the plan maintained by Tesseract in accordance with Article 74 MiCAR.

1.2 Headings used in these Terms are for convenience of reference only and shall not affect the interpretation thereof. The Annexes form an integral part of these Terms; in the event of any conflict or inconsistency between the body of these Terms and any Annex, the provisions of the body of these Terms shall prevail**.**

1.3 The following operational documents and capture forms are incorporated into these Terms by reference and form an integral part of the agreement between the Parties. They are maintained by Tesseract, available through the Compliance App or on request, and updated from time to time; material updates that affect the Client's substantive position are notified under clause 23.1:

- Data Processing Agreement (GDPR Article 28), executed as a separate envelope where Tesseract acts as processor;
- KYB/KYC Procedure; Sanctions Screening Procedure; Wallet Whitelisting Procedure;
- PEP Self-Declaration Form; Source-of-Funds Declaration; Travel Rule self-hosted wallet declaration; CARF corporate self-certification;
- Suitability Statement template; Periodic Statement template;
- Product Information Summary (one per Strategy: USDC Conservative, USDC Advanced, wBTC Advanced, wETH Advanced);
- Wind-Down Plan customer summary.
- Conflicts of Interest Policy, provided to the Client as part of the pre-contractual information package and available through the Compliance App and/or on request.

2. Client classification, eligibility and onboarding

2.1 Corporate Client only. These Terms apply only to Corporate Clients. MiCAR does not impose a client-classification taxonomy, and no MiFID II Retail / Professional / Eligible Counterparty classification applies to these Terms.

2.2 Eligibility. Tesseract may update the hard-block list at any time by publishing a revised list through the Compliance App with at least 14 days' prior notice to existing Clients affected by any addition. Removal of a jurisdiction from the hard-block list takes effect immediately on publication. The current version of the Eligibility List is always accessible through the Compliance App.

- **Eligible jurisdictions (open list):** All EEA Member States (the 27 EU Member States plus Iceland, Liechtenstein and Norway).
- **Hard-block list:** United States, United Kingdom, United Arab Emirates, Japan, Republic of Korea, Singapore and Australia.
- **Sanctions overlay:** Consolidated EU restrictive measures (including Council Regulation (EU) No 269/2014 and related instruments).
- **Enforcement:** Geo-IP block at the marketing layer; eligibility gate at account creation.

2.3 Onboarding, KYB and AML. Prior to the funding of any Vault, the Client shall complete know-your-business (KYB) verification, ultimate beneficial ownership (UBO) identification, sanctions screening, politically exposed persons (PEP) screening, and source-of-funds checks through the Compliance App. Tesseract reserves the right to refuse, suspend or escalate any onboarding application to the Money Laundering Reporting Officer (MLRO) on risk-based grounds. The supporting procedures and document capture forms are set out and referenced in clause 1.3.

2.4 Authorized Persons. The Client designates Authorized Persons in Annex A. The Client may operate on a self-custody basis or through a Client’s Custodian designated by it. Authorized Persons may instruct deposits, withdrawals and operational actions through the Vault Interface, subject always to the applicable wallet-control, whitelisting, signing and custody-side authorization mechanics. Internal Client governance, including dual signature, key custody, allocation of signing authority and any arrangement with a Client’s Custodian, is the Client’s responsibility and does not bind Tesseract beyond the Authorized Person list, the notified custody arrangement and the applicable access-control mechanics.

3. Suitability assessment

3.1 Assessment before service. Prior to the provision of portfolio management services, Tesseract shall conduct a suitability assessment in accordance with Article 81 of MiCAR, gathering from the Client the following

information: (i) knowledge and experience in financial markets, including crypto-assets; (ii) investment objectives and risk tolerance; (iii) financial situation and ability to bear losses; and (iv) understanding of the risks inherent to crypto-assets.

3.2 Structure and outcomes. The suitability assessment comprises two parts:

a) **Part 1 — Test of understanding:** Standard knowledge questions plus DCV-specific questions on (i) smart-contract risk, (ii) leveraged DeFi exposure, (iii) IPOR Fusion dependency, and (iv) unwind timeline. Scoring is automatic, the pass threshold is 4 of 7 on the standard block. A score below the threshold blocks access, and a partial score proceeds with educational materials encouraged.

b) **Part 2 — Corporate-Client questionnaire:** A stepped multi-page form covering knowledge and experience, investment objectives and risk tolerance, financial situation and ability to bear losses, and understanding of crypto-asset risks, scored against the single aggregated DCV target market. All questions are mandatory; save-and-resume with a 30-day expiry is recommended.

c) **Outcomes:**

- Defined target market — proceed (access to all Strategies);
- Outside target market — proceed with logged acknowledgement and warning under clause 3.3;
- Negative target market — hard block with warning under clause 3.3.

3.3 Single high-risk band. All Strategies available in the catalogue fall within the same MiCAR high-risk suitability band and a single aggregated Decentralized Credit Vault (DCV) target market. Accordingly, a Client who successfully completes the suitability assessment shall be entitled to deploy any or all of the available Strategies, without the requirement of a per-Strategy election or individual gating mechanism. A negative target market determination shall constitute a hard block, precluding the Client from proceeding. Where a determination of 'outside target market' is made, Tesseract shall deliver a written warning to the Client before the Client proceeds, clearly stating that Tesseract considers the service to be outside the Client's target market. The Client may nonetheless proceed only following receipt and acknowledgement of such warning, which shall be recorded in the Compliance App audit log and stored as part of the Client's suitability record.**3.4 Reassessment.** Tesseract operates a twelve (12)-month suitability re-confirmation process, as a matter of internal policy. In addition, a triggered reassessment shall be conducted upon any material change in the Client's circumstances.

4. Appointment, scope of services, Vaults and Strategies

4.1 Appointment. The Client appoints Tesseract, and Tesseract accepts the appointment, as the MiCAR-authorised crypto-asset service provider responsible for the services comprised in the DCV model, including custody and administration of crypto-assets on behalf of clients, portfolio management of crypto-assets and transfer services for crypto-assets, in each case as allocated to Tesseract under these Terms. For the avoidance of doubt, as further described in Clause 5, the services provided by Tesseract within the DCV structure may constitute custody and administration of crypto-assets on behalf of clients for the purposes of MiCAR by reason of Tesseract’s control over the dedicated vault structure and its ability to administer, operate and effect transactions in respect of Vault Assets, notwithstanding that the relevant wallet infrastructure, private cryptographic keys or other wallet-level means of access shall be held or controlled by the Client or, where applicable, by the Client’s Custodian. Beneficial ownership and proprietary entitlement to the Vault Assets remain exclusively with the Client at all times.

4.2 Scope of services. Tesseract shall provide: (a) custody and administration of Vault Assets within the DCV operating model and in accordance with the allocation of functions described in clause 5; (b) discretionary management per the Investment Mandate, including deployment into Approved Protocols; (c) transfer services to and from the DCV; (d) a layered risk-control framework (pre-allocation filtering, post-allocation monitoring, and the Guardian Pause); (e) reporting and reconciliation; (f) in accordance with Article 66(3) MiCAR, Tesseract shall provide the Client, in a clear and accessible manner and before the relevant service is provided, with hyperlinks to the crypto-asset white papers relating to the crypto-assets in respect of which Tesseract provides services under these Terms. Such hyperlinks shall be made available through the Compliance App and/or Tesseract's website and kept appropriately up to date; and (g) such other services as the Parties may agree in writing.

4.3 Yield characterization. Any yield generated by deploying Vault Assets into Approved Protocols under the Investment Mandate results from active portfolio-management decisions and does not constitute interest on, or remuneration for the mere holding of, an e-money token within the meaning of Article 50 MiCAR. Tesseract is not an e-money-token issuer and does not offer, pay or promise interest or any other remuneration by reason of the mere holding of any e-money token. Any return associated with a Vault derives from active portfolio management, deployment decisions and participation in DeFi protocols under the Investment Mandate, subject to the risks described in these Terms. Nothing in these Terms, in any Strategy description, in any Product Information Summary, in any marketing communication or in any operational flow shall be interpreted as providing, promising or advertising interest or other remuneration by reason of the mere holding of an e-money token.

4.4 Client Type. The Client confirms that the Client Type recorded in Annex A (self-custody institutional client, or client using its own third-party Custodian) reflects its operational architecture and shall notify Tesseract promptly of any change.

4.5 Multiple Vaults and Strategies. Having passed the suitability assessment, the Client may deploy one or more Vaults across any of the available Strategies. Each Vault operates a single Strategy, and no additional per-Strategy suitability assessment or approval is required**.**

4.6 Strategy per Vault. Each Vault runs a single Strategy, fixed at deployment. To move to a different Strategy, the Client deploys a new Vault running that Strategy (and may redeem from an existing Vault); there is no in-place change of a deployed Vault's Strategy. The Client contracts at the high-level Strategy layer; Tesseract operates the underlying deployment Strategy within the high-level parameters and the Approved Protocols list at its operational discretion, subject to these Terms, the risk disclosures (Annex C) and the Investment Mandate (Annex D). Changes to the underlying deployment Strategy do not change the contracted high-level Strategy.

4.7 Deployment is operational. Deployment of a Vault running an available Strategy is operational: the Authorized Person initiates deployment through the Vault Interface and the corresponding Vault Parameter Sheet (Annex A) populates from the on-chain Vault Deployed event. No fresh acceptance is required for additional Vaults.

4.8 Transparency. Tesseract publishes the live underlying deployment Strategy composition through the Public API (api.vault.tesseract.fi) and the Vault Interface; the Client may inspect it at any time.

5. Custody, ownership and asset control

5.1 Regulatory characterisation. The Parties acknowledge that, for the purposes of MiCAR, the DCV operating model includes the provision by Tesseract of custody and administration of crypto-assets on behalf of clients, together with portfolio management and transfer services, as applicable to the structure operated under these Terms. The Parties further acknowledge that, within the layered custody architecture contemplated herein, the holding or control of the relevant wallet infrastructure, private cryptographic keys, key shards or other means of access may remain with the Client itself or with the Client's Custodian, while Tesseract performs the control, administration, safeguarding, operational and smart-contract functions expressly allocated to it under these Terms.

5.2 Custody model. The custody architecture and Tesseract will not hold any of the Client's private cryptographic keys. Where assets are transferred into the DCV structure, they are held through the Client's individually segregated smart-contract vault, in respect of which Tesseract is granted the operational permissions and control functions necessary to administer the Vault and carry out Deployment Actions within the agreed mandate. At all times, the Client retains the beneficial interest in the Vault Assets, and Tesseract does not acquire legal or beneficial title to the Vault Assets.

5.3 Role of Tesseract. Tesseract acts as the MiCAR-authorised service provider for the services comprised in the DCV model, including custody and administration of crypto-assets on behalf of clients to the extent applicable to the dedicated-vault structure operated under these Terms. Tesseract's role includes the control, administration and operation of the DCV smart-contract structure, the execution of Deployment Actions, the implementation of the agreed investment mandate, the performance of transfer-related functions and the maintenance of the safeguarding, segregation and record-keeping framework applicable to the Vault Assets. Tesseract does not hold the Client's private cryptographic keys except where expressly agreed in writing under a separate custody arrangement.

5.4 Role of the Client and of the Client's Custodian. The Client remains responsible for its chosen wallet architecture. Where the Client designates a Client's Custodian, that provider performs the key-custody, wallet-control and custody-side authorisation functions allocated to it within the layered custody model, including holding or controlling the relevant private cryptographic keys, key shards or other means of access. The

applicable signing threshold, wallet-control framework and approval mechanics are agreed between the Client and the Client's Custodian and shall be notified to Tesseract to the extent operationally relevant. Tesseract cannot unilaterally move assets out of the Client's or the Client's Custodian's wallet infrastructure except through the operational mechanisms expressly contemplated by the DCV structure and these Terms.

5.5 Asset segregation, records and traceability. In accordance with Article 75 MiCAR, Tesseract shall maintain records sufficient to identify the Client's Vault Assets across the relevant layers of the DCV structure, including the dedicated vault, deployed protocol positions and any yield-bearing equivalents or transformed positions arising from deployment activity. Each Vault is dedicated to a single Client and operates without pooling or commingling with other client assets.

5.6 Asset flows and operational control. The operational asset flow is as follows: (a) on the Client's instruction and subject to the applicable wallet, whitelisting and custody controls, assets move from the relevant wallet infrastructure of the Client or its Client's Custodian to the DCV for deployment under the Investment Mandate; (b) while deployed, Tesseract manages strategy execution within the DCV and across Approved Protocols in accordance with these Terms; and (c) on redemption, unwind, Guardian Pause, termination or other authorised return event, assets are withdrawn or reconverted as necessary and returned in accordance with the agreed wallet, custody and settlement flow, including to the Client or its Client's Custodian, as applicable.

5.7 Asset transformation. Deployment into DeFi protocols may transform the original asset into yield-bearing equivalents (for example, USDC into USDC). Such transformation is not a disposal or consumption of the Client's assets, the relevant yield-bearing tokens represent a continuing exposure or claim within the deployed strategy, and the Client's beneficial interest is maintained throughout, subject to the risks of the relevant protocol and asset structure.

5.8 No rehypothecation or proprietary use. In accordance with Article 75(2) MiCAR, Tesseract shall not rehypothecate, pledge, encumber or otherwise use Vault Assets for its own account or for the account of any third party, and shall not grant any security interest, lien or charge over Vault Assets except as expressly authorised by the Client in writing or as strictly required for the execution of the services under these Terms.

5.9 Asset transformation. Deployment into DeFi protocols may transform the original asset into yield-bearing equivalents (e.g. USDC into USDC). Such transformation is not a disposal or consumption of the Client's assets; the yield-bearing tokens represent a continuing claim, and the Client's beneficial ownership is maintained throughout.

5.10 Tracing and identification. In accordance with Article 75(1) MiCAR, Tesseract shall maintain separate accounting records distinguishing the Client's assets from those of any other client and from Tesseract's own assets, and records sufficient to trace all yield-bearing tokens, derivative positions and protocol allocations back to the originating DCV.

5.11 Vault Tokens. Vault Tokens represent the Client's contractual and on-chain claim in respect of the DCV's holdings. They are non-transferable, shall not be traded or listed, and do not constitute a financial instrument, transferable security or unit in a collective investment undertaking.

5.12 Reconciliation and insolvency interface. Tesseract shall reconcile the Client's asset position across the relevant custody and deployment layers in accordance with clause 9.4. The insolvency protections in clause 6 apply across the custody architecture described in this clause, and in a wind-down scenario the operational arrangements shall be applied so as to support the orderly return or redemption of Vault Assets in accordance with these Terms.

6. Insolvency protections

6.1 Segregation and right of separation. The Parties acknowledge that each DCV forms part of a layered custody architecture in which the Client retains beneficial ownership of the Vault Assets at all times and Tesseract does not acquire any legal or beneficial title to the Vault Assets by reason only of its control and administration functions within the DCV. Vault Assets are segregated from Tesseract's proprietary assets and, in accordance with Article 75(7) MiCAR, shall not form part of Tesseract's insolvency estate or be available to its creditors. Tesseract shall maintain contemporaneous records sufficient to identify each Client's Vault Assets at DCV and protocol level. To the extent applicable under Finnish insolvency law, including Chapter 5, Section 6 of the Finnish Bankruptcy Act, the Client shall assert a right of separation in respect of the Vault Assets.

6.2 Guardian Pause and Suspension Events. Tesseract may activate the Guardian Pause to halt Deployment Actions or redemption processing exclusively on: (a) a Force Majeure Event (Clause 22) affecting the DCV; (b) regulatory action by FIN-FSA or another competent authority; (c) a material market-disruption event at an Approved Protocol (protocol insolvency, smart-contract exploit, oracle failure, liquidity crisis) where continued

execution would expose Vault Assets to material risk of loss; or (d) a compliance event (AML flag, sanctions alert, Travel Rule deficiency or other compliance hold). General market conditions, including price volatility, are expressly excluded as a trigger.

6.3 Notification. Tesseract shall notify the Client of any Guardian Pause within two Business Days in the case of categories (a), (b) and (d), and within one Business Day in the case of category (c), specifying the category, reason, scope and expected duration. In a winding-down scenario, the Guardian Pause shall be lifted to allow the Client direct on-chain access to redeem Vault Tokens, subject to the availability of liquidity in the underlying protocols. In accordance with Article 74 MiCAR, a summary of Tesseract's Wind-Down Plan is always made available to the Client through the Compliance App and/or on Tesseract's website. The full Wind-Down Plan is maintained and updated by Tesseract and submitted to the competent authority as required by Applicable Law. In a wind-down scenario, Tesseract shall notify the Client as soon as reasonably practicable and shall implement the Wind-Down Plan so as to support the orderly unwind, return or redemption of Vault Assets through the custody architecture described in clause 5**.**

7. Fees and VAT

7.1 Fee schedule. The Client shall pay the Fees set out in Annex A. The standard schedule applies to all Strategies unless varied by a per-Vault commercial overlay recorded in the relevant Vault Parameter Sheet.

7.2 Crystallization and high-water mark. Performance crystallization events are any redemption (full or partial), the end of each calendar quarter, and termination. Performance fee is charged only on the increase above the highest Vault Token Price at any prior crystallization event; the high-water mark resets on termination or full redemption.

7.3 Fee deduction mechanism. Fees are satisfied through a proportional reduction in the Client's claim on the underlying Vault Assets, and not through any seizure or appropriation of Vault Assets. The reduction may be effected on-chain by either (a) a proportional burn of the Client's Vault Tokens corresponding to the value of the Fees due, or (b) the equivalent mint-and-redeem mechanism, by which Vault Tokens corresponding to the value of the Fees due are minted to a Tesseract fee account and subsequently harvested and redeemed by Tesseract for Vault Assets. Both mechanisms produce the same economic effect on the Client's proportional claim. The Vault Interface discloses the mechanism applied and the number of Vault Tokens reduced or minted in respect of each Fee deduction. Harvest is aligned operationally with the crystallization events in clause 7.2.

7.4 Gas and transaction costs. The Client bears gas on Client-initiated transactions (Vault creation, deposits) from the Whitelisted Address, swap costs, slippage incurred in the course of rebalancing within the Vault, and transaction costs. Tesseract absorbs gas on Tesseract-initiated management transactions undertaken in the discharge of the discretionary management mandate.

7.5 Fee changes and disputes. Tesseract may change the fee schedule on 30 days' notice; the Client may terminate without penalty if the change is unacceptable and unjustified. Fee disputes must be notified within 30 days of the relevant statement; pending resolution the full amount remains due, with prompt refund or credit of any overpayment.

7.6 VAT. The Fees are stated exclusive of value added tax (VAT) and any equivalent indirect tax. Tesseract shall invoice the services in accordance with the VAT treatment that it determines in good faith to be applicable under Applicable Law, acting on the basis of its tax analysis and, where appropriate, external tax advice. Where Tesseract determines that VAT is chargeable in respect of any Fee, it may charge VAT in addition to that Fee with effect from the date required by Applicable Law or, where later, from the date on which Tesseract begins applying that treatment. Where the reverse-charge mechanism or any other customer-accounting mechanism applies, the Client shall account for VAT accordingly. The Client remains responsible for its own tax position, filings and payments under Applicable Law, and Tesseract does not provide tax advice**.**

> **7.7 Public fee disclosure**. In accordance with Article 66(4) MiCAR, Tesseract publishes, and keeps appropriately updated, information on its pricing, costs and fees in a prominent place on its website and through the Compliance App. The fee schedule applicable to the Client under these Terms is set out in Annex A and, where applicable, the relevant Vault Parameter Sheet.

8. Deposit, redemption and whitelisting

8.1 Deposit. The Client deploys Vault Assets through the custody and wallet architecture described in clause 5. Subject to the applicable wallet-control, whitelisting, Travel Rule and compliance requirements, assets are transferred from the relevant wallet infrastructure of the Client or its Client's Custodian, or from another permitted originating wallet, to the DCV for deployment under the Investment Mandate. Upon receipt at the DCV smart-contract address, the corresponding Vault Tokens are minted to the Client or to the relevant

Whitelisted Address, as applicable. Each deposit remains subject to the controls and verifications described in these Terms, and nothing in this clause shall be interpreted as giving Tesseract custody of the Client's private keys.

8.2 Redemption Notice. The Client may at any time submit a signed, on-chain Redemption Notice through the Vault Interface to redeem all or part of the Vault Assets. The redemption executes on-chain automatically, subject to market and liquidity conditions and the suspension rights below, no Tesseract approval step is required in normal operation.

8.3 Suspension. Tesseract may suspend or delay a redemption only on a Suspension Event (clause 6.2) or where execution would cause Tesseract to breach Applicable Law, notifying the Client without undue delay.

8.4 Proceeds and costs. Redeemed Vault Assets are transferred to the wallet or address designated by the Client or, where applicable, its Client's Custodian. Proceeds may be reduced by the unwind cost incurred at the underlying Strategy layer (gas, slippage, swap fees) as disclosed in Annex A and the relevant Vault Parameter Sheet. Withdrawal settlement: T+1 for USDC Conservative; T+2 (target) for each Advanced Strategy, which may be extended based on market conditions. Under certain conditions, withdrawals may experience delays.

8.5 Whitelisting. The Client maintains a list of Whitelisted Addresses, established at onboarding via the Compliance App, and may add, remove, or modify an address by signed instruction from an Authorized Person, effective on Tesseract's confirmation. A Whitelisted Address may belong to the Client or, where applicable, to the Client's Custodian, provided that the relevant ownership, control and compliance requirements are satisfied. Registration of the Whitelisted Address on the on-chain Whitelisting Contract is a condition precedent to any deposit, but not to acceptance of these Terms. The whitelisting procedure is referenced in Clause 1.3.

9. Reporting and reconciliation

9.1 Real-time access. Tesseract provides real-time access via three independent surfaces, any of which the Client may use without Tesseract's per-call involvement: (a) on-chain ERC-4626 reads on the Vault contract; (b) the Public API at api.vault.tesseract.fi (vault discovery, decoded transaction history, performance time-series, current Strategy assignment); and (c) the Compliance App dashboard (Vault state, Vault Token Price, allocations, transaction history, accrued fees, KYC and whitelisting status).

9.2 Live versus on-touch valuation. The Vault's on-chain total Assets value (and the Vault Token Price derived from it) updates only on a transaction that touches the Vault (deposit, withdrawal, rebalance, fee accrual). Between such transactions on-chain figures may be stale relative to the live value of the underlying positions; the Public API publishes snapshots simulating live valuations and is the canonical source for live performance figures.

9.3 Periodic statement. Tesseract issues a Periodic Statement each calendar quarter, within 30 days of quarter-end, on a durable medium by email and through the document drawer, with a version hash recorded in the audit log. Minimum content: (a) account and Vault identification; (b) Vault valuation and NAV methodology; (c) performance (gross and net, trailing 12 months and inception-to-date, attribution drivers); (d) positions and allocations across Approved Protocols and the Strategy in force; (e) activity (deposits, withdrawals, rebalances, de-risking actions); (f) fees and charges (management and performance fees, informational gas costs); (g) conflicts and inducements with reference to the Conflicts Policy; (h) suitability re-confirmation; (i) material events and a reconciliation of Vault Assets; and (j) a reminder of principal risks (Annex C), that yields are indicative not guaranteed, and a DAC8 tax-information statement. The Client may request an on-demand statement at any time through the Compliance App.

9.4 Reconciliation. Tesseract reconciles the Client's asset position across the relevant custody and deployment layers in accordance with clause 5.10, including the dedicated vault, deployed protocol positions and any relevant yield-bearing equivalents or transformed positions. The Client may also reconcile against on-chain state at any time to the extent technically available. Discrepancies may be raised through the Compliance App or to support@tesseract.fi and are triaged under Tesseract's support and incident-response framework**.**

10. Travel Rule and AML

10.1 Travel Rule data exchange. In accordance with Regulation (EU) 2023/1113, the Client shall, for each deployment and redemption, provide all required originator and beneficiary information (including the identity and wallet address of originator and beneficiary, and counterparty wallet-provider data) via the Compliance App or Vault Interface. Tesseract transmits, receives and retains such information in accordance with Applicable Law.

10.2 Sanctions screening and self-hosted wallets. Tesseract performs sanctions screening on all wallet addresses involved, including unhosted (self-hosted) addresses, using the tools integrated into the Compliance App. Where the Client uses a non-custodial wallet provider it shall provide a self-hosted-wallet declaration (referenced in Clause 1.3). Tesseract may refuse or suspend any transfer where required Travel Rule information is missing, screening is positive or inconclusive, or self-hosted verification is incomplete; such refusal is not a breach.

10.3 Warranties and liability. The Client warrants that all Travel Rule information is accurate, complete and not misleading, and shall indemnify Tesseract against losses arising from any inaccuracy. Tesseract may freeze the DCV, suspend Deployment Actions or restrict access where the Client fails to provide required information, the information is materially inaccurate, or Tesseract reasonably believes processing would breach Applicable Law; any such action is a Suspension Event.

10.4 Ongoing monitoring and additional information. Tesseract may, at any time during the term of these Terms, require the Client to provide additional information, documents, explanations or supporting evidence in connection with any deposit, redemption, transfer, wallet, beneficial owner, source of funds, source of wealth, counterparty, transaction pattern or jurisdictional nexus where Tesseract reasonably considers such information necessary or appropriate for compliance with Applicable Law, internal AML/CFT procedures, sanctions controls, Travel Rule obligations, fraud prevention, risk management or any request from a competent authority. The Client shall provide such information promptly and, in any event, within the timeframe reasonably specified by Tesseract.

10.5 Refusal, blocking and reporting. Tesseract may refuse, delay, block, return, freeze, suspend, restrict or report any deposit, redemption, transfer, instruction, wallet or Vault activity where Tesseract reasonably determines, suspects or is advised that: (a) the relevant activity may breach Applicable Law; (b) the Travel Rule information is missing, incomplete, inconsistent or inaccurate; (c) sanctions, AML/CFT, fraud, tax-reporting or law-enforcement concerns arise; (d) the relevant wallet, protocol, asset, jurisdiction, counterparty or transaction pattern presents elevated legal, regulatory, operational or reputational risk; or (e) a filing, disclosure, escalation, suspicious-transaction report or other report to a competent authority is required or appropriate. To the extent permitted by Applicable Law, Tesseract may refrain from disclosing the grounds for any such action where disclosure would be unlawful or would prejudice an investigation, report or compliance review.

10.6 No liability for compliance action. Any action or omission by Tesseract in good-faith compliance with Applicable Law, sanctions obligations, AML/CFT obligations, Travel Rule requirements, internal compliance procedures or a request, order, notice or expectation of a competent authority shall not constitute a breach of these Terms and shall not give rise to liability on the part of Tesseract, except in the case of fraud, wilful misconduct or gross negligence.

10.7 Client cooperation. The Client shall cooperate fully and in good faith with all compliance, AML/CFT, sanctions, Travel Rule, fraud-prevention and regulatory-review measures operated by Tesseract from time to time, including enhanced due diligence, remediation requests, re-screening, wallet verification, source-of-funds/source-of-wealth review, tax self-certification refresh and remediation of incomplete or outdated information. Failure to cooperate within the timeframe reasonably specified by Tesseract constitutes a material breach and a Suspension Event.

11. Data protection and roles

11.1 Compliance and roles. Each Party shall comply with the GDPR. Tesseract processes personal data as an independent controller where necessary for the provision of regulated services, compliance with legal obligations (AML/CFT, sanctions, fraud prevention, Travel Rule) and risk-management/operational-resilience obligations. Where Tesseract processes data strictly on the Client's documented instructions it acts as processor under Article 28 GDPR and the Parties shall enter into the data-processing agreement referenced in Clause 1.3 before such processing.

11.2 Third parties, breach, data-subject rights. Tesseract may rely on third-party providers (identity verification, compliance monitoring, blockchain analytics, cloud, security) acting as independent controllers or as processors bound by Article 28 GDPR and, where applicable, DORA. Each Party shall notify the other of any personal-data breach without undue delay (immediately where Tesseract is processor) with information sufficient to meet Articles 33–34 GDPR. The Parties shall cooperate on data-subject requests under Chapter III GDPR. Where automated processing (transaction monitoring, AML screening) produces legal or similarly significant effects, the data subject may obtain human intervention, express their view and contest the decision.

11.3 International transfers. To the extent that personal data is transferred outside the European Economic Area or otherwise to a jurisdiction not benefiting from an adequacy decision, the transferring Party shall ensure

that such transfer is subject to an appropriate transfer mechanism recognised under Applicable Law, including the European Commission's standard contractual clauses where required, together with any supplementary measures reasonably necessary in the circumstances.

11.4 Retention. Tesseract may retain personal data for so long as necessary for the purposes for which it was collected and processed, including the provision of services, performance of these Terms, auditability, incident response, dispute management, exercise or defence of legal claims, AML/CFT and sanctions compliance, Travel Rule compliance, tax reporting, record-keeping under MiCAR, DORA and other Applicable Law, and the satisfaction of regulatory retention periods.

11.5 Security measures. Each Party shall implement and maintain appropriate technical and organisational measures designed to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, taking into account the nature of the data, the state of the art, the costs of implementation, the context and purposes of processing, and the risks to the rights and freedoms of natural persons.

11.6 Processor assistance and audit limitations. Where Tesseract acts as processor, it shall provide reasonable assistance to the Client in relation to data-subject requests, personal-data-breach management, data-protection impact assessments and regulator engagement, in each case to the extent required by Article 28 GDPR and proportionate to the nature of the processing. Any audit or information request by the Client in that capacity shall be exercised on reasonable prior notice, during normal business hours, subject to confidentiality safeguards, and without unreasonably interfering with Tesseract's operations, security framework or obligations to other clients.

11.7 Survival. This clause shall survive termination for so long as either Party continues to process personal data obtained in connection with these Terms.

12. Representations, warranties and regulatory acknowledgments

12.1 Mutual. Each Party represents and warrants that it has full power and authority to enter into and perform these Terms, that execution has been duly authorized, that these Terms are legal, valid, binding and enforceable; that performance will not violate Applicable Law or any third-party obligation, and that it is not insolvent. Each Party shall promptly notify the other of any regulatory inquiry, investigation or enforcement relating to these Terms.

12.2 Tesseract. Tesseract further warrants that it: (a) is duly authorised by the FIN-FSA as a CASP under MiCAR and maintains all required licences, registrations and regulatory approvals for the services it provides under these Terms; (b) maintains adequate arrangements for the safeguarding, administration, segregation, traceability and operational control of Vault Assets within the DCV operating model and in accordance with the allocation of functions described in clause 5 and Article 75 MiCAR; (c) does not hold the Client's private keys except to the extent, if any, expressly agreed in writing under a different custody arrangement not governed by these Terms; (d) maintains a Wind-Down Plan in accordance with Article 74 MiCAR; and (e) maintains permanent minimum capital in compliance with applicable MiCAR requirements, being no less than EUR 125,000 or one quarter of its preceding year's fixed overheads, whichever is higher, it being acknowledged that such capital requirement constitutes a firm-level solvency buffer and not a loss-absorption mechanism for Client investment losses**.**

12.3 Client. The Client warrants that: (a) it possesses the requisite knowledge, experience and expertise to independently evaluate the risks associated with the services provided hereunder, and has conducted its own independent assessment without reliance on any recommendation made by Tesseract; (b) the Vault Assets are beneficially owned by the Client or, alternatively, the Client holds full authority to deploy such assets and grant the Investment Mandate; (c) where the Client uses a Client's Custodian or other third-party custody infrastructure, the Client has full authority to designate that provider and to instruct the use of the relevant wallet, signing and settlement arrangements in connection with these Terms; (d) the deployment of Vault Assets does not violate any agreement, obligation or fiduciary duty binding upon the Client; and (e) the Client classification and custody set-up recorded in Annex A are accurate and complete as of the date of these Terms.

12.4 Sanctions. Each Party warrants, on the Effective Date and continuously, that neither it nor its directors, officers, employees, agents or (for the Client) beneficial owners or controlling persons is the subject of, or controlled by a person subject to, Sanctions administered by the UN, EU, US (OFAC), UK (OFSI) or Finland; that it is not based in a Sanctioned Jurisdiction; and that it will comply with all applicable Sanctions, AML/CFT, anti-bribery and anti-corruption laws and will not use Vault Assets to fund or facilitate any activity with a sanctioned person or jurisdiction.

12.5 AML/CFT and source of funds. The Client acknowledges Tesseract's KYC/KYB, transaction-monitoring and suspicious-activity-reporting obligations and warrants that its funds are lawfully derived and not proceeds of crime, that it is not sanctioned or listed, and that all onboarding information is accurate. The Client shall cooperate with ongoing and enhanced due diligence and respond to information requests within ten Business Days. Tesseract may freeze the DCV, suspend Deployment Actions, restrict access or terminate where suspicious patterns are detected, the Client is sanctions-listed, the Client fails to cooperate, a regulator requests an asset freeze, or Applicable Law requires.

12.6 Tax reporting (DAC8 / CARF). The Client acknowledges Tesseract's reporting obligations under Directive (EU) 2023/2226 (DAC8) and the OECD Crypto-Asset Reporting Framework, as transposed into Finnish law, including reporting to the Finnish Tax Administration. The Client shall provide accurate tax-identification information (corporate self-certification referenced in Clause 1.3) and notify changes within 30 days. The Client is solely responsible for its own tax obligations.

12.7 Digital operational resilience (DORA). Tesseract is subject to Regulation (EU) 2022/2554 (DORA) and maintains an ICT risk-management framework, classification and reporting of major ICT incidents to FIN-FSA (Articles 17–23 DORA) with client notification of incidents materially affecting the DCV, ICT testing, business-continuity and disaster-recovery plans, and a register of third-party ICT providers with due diligence on critical providers (Articles 28–30 DORA).

13. RISK ALLOCATION

13.1 INVESTMENT RISK. THE CLIENT ACCEPTS THAT ALL INVESTMENT RISK (INCLUDING DEFI PROTOCOL, SMART-CONTRACT, LIQUIDITY, MARKET, LEVERAGE, STABLECOIN DE-PEG, ORACLE AND REGULATORY RISK) IS BORNE BY THE CLIENT AND ACKNOWLEDGES THE COMPREHENSIVE RISK DISCLOSURES IN ANNEX C. THE DCV IS NOT A SWAP, COUNTERPARTY ARRANGEMENT OR GUARANTEE; TESSERACT DOES NOT GUARANTEE ANY RETURN, YIELD OR THE PRESERVATION OF PRINCIPAL.

13.2 SMART-CONTRACT AND PROTOCOL FAILURE. LOSSES ARISING FROM SMART-CONTRACT FAILURE, DEFI PROTOCOL FAILURE OR PROTOCOL-LEVEL INSOLVENCY ARE BORNE BY THE CLIENT, SAVE TO THE EXTENT DIRECTLY ATTRIBUTABLE TO TESSERACT'S NEGLIGENCE IN SELECTING, MONITORING OR REMOVING THE RELEVANT APPROVED PROTOCOL, OR TO ITS FRAUD, WILLFUL MISCONDUCT OR GROSS NEGLIGENCE.

13.3 NO ADVICE. THE CLIENT ACKNOWLEDGES AND AGREES THAT, EXCEPT TO THE EXTENT EXPRESSLY STATED OTHERWISE IN THESE TERMS, TESSERACT DOES NOT PROVIDE LEGAL, TAX, ACCOUNTING OR INVESTMENT ADVICE TO THE CLIENT AND DOES NOT ACT AS THE CLIENT'S FIDUCIARY BEYOND THE SPECIFIC CONTRACTUAL AND REGULATORY DUTIES EXPRESSLY ASSUMED UNDER THESE TERMS. THE CLIENT HAS MADE, AND SHALL CONTINUE TO MAKE, ITS OWN INDEPENDENT ASSESSMENT OF THE SUITABILITY, LEGALITY, TAX TREATMENT, ACCOUNTING TREATMENT, ECONOMIC MERITS AND RISKS OF THE SERVICES, THE DCV STRUCTURE, THE STRATEGIES, THE APPROVED PROTOCOLS AND THE SUPPORTED ASSETS, AND IS NOT RELYING ON ANY STATEMENT, COMMUNICATION, PROJECTION, MARKETING MATERIAL OR EXPECTATION OTHER THAN THE EXPRESS TERMS OF THE CONTRACTUAL DOCUMENTATION AND THE MANDATORY INFORMATION DELIVERED UNDER APPLICABLE LAW**.**

14. Limitation of liability

14.1 Exclusions. To the maximum extent permitted by Applicable Law, neither Party is liable for indirect, special, incidental, consequential or punitive damages, including loss of profits, revenue, business opportunity or data.

14.2 Cap. Tesseract's aggregate liability under or in connection with these Terms shall not exceed the total Fees paid by the Client in the six (6) months immediately preceding the date the relevant claim is first asserted in writing, this clause shall be read jointly with clause 14.4.

14.3 Passive breach. Market movements, liquidations or involuntary rebalancing may cause the DCV temporarily to breach the Investment Mandate parameters. Such passive breaches are not a breach entailing Tesseract liability if Tesseract actively works to restore compliance within 48 hours, Tesseract is not required to liquidate at unfavorable prices to immediately cure them.

14.4 Carve-outs. The exclusions and cap do not apply to: (a) fraud, willful misconduct or gross negligence; (b) breach of the custody and segregation obligations in clauses 5 and 6; (c) breach of confidentiality under clause 16; or (d) any liability that cannot be limited or excluded under Applicable Law.

14.5 Duty to mitigate. Each Party shall take reasonable steps to mitigate any loss, cost or damage suffered or incurred in connection with any claim under or relating to these Terms.

14.6 Time limit for claims. No claim arising out of or in connection with these Terms may be brought by the Client more than twelve (12) months after the date on which the Client became aware, or ought reasonably to have become aware, of the facts giving rise to the claim, save where a longer period is mandatorily required by Applicable Law.

14.7 Third-party infrastructure and external dependencies. Without prejudice to the carve-outs in clause 14.4, Tesseract shall not be liable for any loss, delay, failure, inaccuracy, unavailability or adverse consequence arising from or connected with: (a) any blockchain, validator, sequencer, oracle, bridge, RPC provider, smart-contract system, DeFi protocol, custody provider, cloud provider, telecommunications provider, internet-service provider, identity provider, compliance vendor or other third-party system or dependency; (b) congestion, conditions, chain reorganisation, MEV effects, malfunction, protocol governance action, bridge failure, wallet compromise outside Tesseract's control, or any incompatibility between third-party infrastructure components; or (c) any act or omission of the Client, an Authorized Person, the Client's Custodian or any other third party acting for or through the Client.

14.8 Operation of this clause. The limitations, exclusions and allocations of risk in these Terms reflect the agreed commercial allocation of risk between the Parties and apply to all causes of action, whether in contract, tort (including negligence), breach of statutory duty, misrepresentation, restitution or otherwise, to the fullest extent permitted by Applicable Law.

15. Indemnification

15.1 By Tesseract. Tesseract shall indemnify the Client and its directors, officers, employees and agents against losses arising from: (a) any material breach by Tesseract of these Terms; (b) Tesseract's negligence, wilful misconduct or fraud; (c) any failure by Tesseract to comply with Applicable Law in connection with the services allocated to it under these Terms; or (d) any breach by Tesseract of its obligations relating to segregation, safeguarding, record-keeping, reconciliation, operational control or the non-proprietary treatment of Vault Assets within the custody architecture described in clause 5**.**

15.2 By the Client. The Client shall indemnify Tesseract and its directors, officers, employees and agents against losses arising from any material breach by the Client; any inaccuracy in information provided (including Travel Rule information); or any failure by the Client to comply with Applicable Law.

15.3 Procedure. The indemnified party shall promptly notify the indemnifying party, which may assume control of the defense with counsel of its choice; the indemnified party may participate at its own cost; no settlement without the indemnified party's consent (not to be unreasonably withheld).

16. Confidentiality

16.1 Each Party shall hold the other's Confidential Information (including the terms of these Terms, technical data, know-how, business plans, financial and client information, and proprietary technology) in confidence and protect it with at least a reasonable degree of care.

16.2 Confidential Information. Confidential Information excludes information that is or becomes public other than by breach, was known before disclosure, is independently developed, or is received from a third party not under a confidentiality obligation.

16.3 Permitted internal disclosure. A Party may disclose Confidential Information to its Affiliates and to its and their directors, officers, employees, professional advisers, auditors, insurers, financing sources, subcontractors and service providers on a strict need-to-know basis, provided that the receiving persons are bound by confidentiality obligations no less protective than those set out in these Terms or are otherwise subject to professional or statutory duties of confidentiality.

16.4 Return, deletion and retention. Upon termination of these Terms or upon reasonable written request by the Disclosing Party, the Receiving Party shall, subject to Applicable Law, regulatory retention duties, internal backup procedures and legitimate record-keeping requirements, return or securely destroy the Confidential Information of the Disclosing Party in its possession or control. Notwithstanding the foregoing, the Receiving Party may retain copies to the extent required for compliance, audit, legal, evidential, dispute-management, business-continuity or cybersecurity purposes.

16.5 Equitable relief. Each Party acknowledges that an unauthorised use or disclosure of Confidential Information may cause irreparable harm for which damages may be an inadequate remedy. Accordingly, the

Disclosing Party is entitled to seek injunctive relief, specific performance or other equitable relief in addition to any other remedies available at law or under these Terms.

16.6 Publicity. Neither Party shall issue any press release or make any public announcement referring to the other Party, the existence of these Terms or the nature of the relationship between the Parties without the prior written consent of the other Party, except where disclosure is required by Applicable Law or by a competent authority.

16.7 Survival. The confidentiality clause survives the termination of the Terms for three (3) years.

17. Conflicts of interest

17.1 Tesseract maintains a conflicts-of-interest policy under Article 72 MiCAR and acts at all times in the best interest of the Client. A summary of how Tesseract identifies, prevents, manages and discloses conflicts is published and is available on request. Any revenue-share paid to a distribution partner is paid out of Tesseract's Fees and is not deducted from the Vault, it is disclosed in the marketing material that introduced the Client to the service. There is no commingling and no undisclosed cross-subsidy between Tesseract's own account and Client Vaults.

17.2 Tesseract's conflicts-of-interest policy, maintained in accordance with Article 72 MiCAR, is provided to the Client as part of the pre-contractual information package delivered through the Compliance App before the Effective Date and is available at all times through the Compliance App and on Tesseract's website. The policy identifies the types of conflicts that exist or may arise between Tesseract, including its management, employees and tied agents, and its clients, or between clients, in connection with the services under these Terms.

17.3 The principal conflicts identified include: (a) Tesseract's own proprietary positions in Supported Assets; (b) revenue-sharing arrangements with distribution partners; and (c) fee structures that may incentivise higher-risk deployments. Where organisational or administrative arrangements are not sufficient to ensure, with reasonable confidence, that risks of damage to the Client's interests will be prevented, Tesseract shall clearly disclose the nature and/or source of the relevant conflict to the Client before acting.

17.4 The Client confirms, by accepting these Terms, that it has received, read and understood the Conflicts of Interest Policy and the summary disclosure in this clause 17, including the principal conflicts identified in clause 17.3(a)–(c), before the Effective Date. The Client's acknowledgement is recorded in the Compliance App audit log.

18. Complaints handling

18.1 Procedure. Tesseract operates a complaints-handling procedure under Article 71 MiCAR. To submit a complaint, contact support@tesseract.fi with the subject line "Formal Complaint". Tesseract acknowledges receipt within five **(5) Business Days**. Tesseract provides a substantive written response within **15 Business Days** of receipt of the complaint. Where, exceptionally, the complaint cannot be resolved within that period for reasons beyond Tesseract's reasonable control or because the matter is complex, Tesseract shall inform the Client before the expiry of that period of the reasons for the delay and of the expected response date, which shall in any event not exceed thirty (30) Business Days from receipt of the complaint**.**

18.2 Escalation. If dissatisfied, the Client may refer the matter to FIN-FSA. The Client's right to bring legal proceedings is unaffected.

18A. Whistleblowing and internal reporting

Tesseract maintains an internal whistleblowing and incident-reporting channel in accordance with Article 71 MiCAR and Articles 17–23 DORA. Employees, contractors and clients may report suspected breaches of MiCAR, DORA or other Applicable Law through the channel published on Tesseract's website and the Compliance App. Reports may be made anonymously where permitted by Finnish law. Tesseract shall not retaliate against any person making a good-faith report. Reports relating to the DCV or the Client's Vault may also be submitted to FIN-FSA directly.

19. Investor compensation and absence of guarantee

19.1 No compensation scheme. Crypto-asset services and crypto-asset holdings provided or administered under these Terms are not covered by the Finnish Investor Compensation Scheme, the Finnish Deposit Guarantee Scheme or any equivalent deposit-protection, investment-protection or statutory compensation arrangement, unless expressly stated otherwise by Tesseract in writing pursuant to Applicable Law.

19.2 No insurance or capital protection. Unless expressly agreed in writing, the services and the Vault Assets are not protected by any capital guarantee, principal-protection undertaking, yield guarantee or investment-

insurance arrangement. Tesseract does not guarantee the return of principal, any minimum value, any level of liquidity, or any target or projected yield.

19.3 Consequences of insolvency or disruption. The Parties acknowledge that, although the contractual and operational model is intended to preserve segregation, traceability and the Client's beneficial interest in Vault Assets, the insolvency of Tesseract, a Client's Custodian, a protocol participant or another relevant third party, or any major operational or legal disruption affecting the DCV structure, may result in delay, impairment, enforcement friction, increased costs, restricted access, forced unwind, valuation uncertainty or partial or total loss.

19.4 No prudential absorption of investment losses. Any prudential-capital, own-funds or governance requirements applicable to Tesseract under MiCAR, DORA or other Applicable Law are firm-level regulatory requirements and do not constitute a reserve, guarantee fund, insurance arrangement or loss-absorption mechanism for the benefit of the Client in respect of investment, protocol, market, technology or counterparty losses.

20. Sustainability disclosure

In accordance with Article 66(5) MiCAR and Commission Delegated Regulation (EU) 2024/2810, Tesseract publishes, in a prominent place on its website and through the Compliance App, information on the principal adverse impacts on the climate and other environment-related adverse impacts of the consensus mechanism used to issue each Supported Asset, covering the six sustainability indicators required by the applicable regulatory technical standards: (i) energy consumption; (ii) greenhouse gas emissions; (iii) renewable energy use; (iv) natural resource consumption; (v) waste production; and (vi) significant impact on biodiversity and ecosystems. This information is published per Supported Asset (USDC, wETH, wBTC) and updated in accordance with the applicable RTS update cycle. The Client may access the current sustainability disclosures at any time through the Compliance App or on request.

21. Term and termination

21.1 Term. These Terms commence on the Effective Date and continue for an initial period of one year, renewing automatically for successive 12-month periods unless either Party gives at least 30 days' written notice of non-renewal before the end of the then-current term.

21.2 For cause. Either Party may terminate immediately on written notice if the other commits a material breach uncured for 30 days, an Insolvency Event occurs, the other's required regulatory authorization is revoked, suspended or materially restricted, or any law or order renders unlawful the performance of a material part of these Terms.

21.3 For convenience. Either Party may terminate at any time on not less than 90 days' prior written notice.

21.4 Effect. On termination, Tesseract shall coordinate the orderly unwind and return of Vault Assets through the custody architecture described in clause 5, including withdrawal or reconversion from deployed positions where applicable, with return to the Client or the Client's Custodian in accordance with the agreed custody and settlement flow. Such return shall be effected as soon as reasonably possible and in any event within 30 Business Days, subject to underlying DeFi liquidity, protocol conditions and abnormal market circumstances. Accrued Fees become immediately due. Tesseract shall provide a final report and reconciliation, including cryptographic or on-chain verification of the relevant return transfers where available. Vault Assets shall remain subject to segregation throughout the wind-down process. Where the Client fails to provide return instructions within 30 days, Tesseract shall continue to safeguard and administer the return process in accordance with Applicable Law and the Wind-Down Plan. Tesseract shall not be liable for any diminution in value of Vault Assets during any safeguarding or return period to the extent attributable to market movements, protocol conditions or external custody-layer constraints outside Tesseract's reasonable control.

21.5 Survival. Clauses 5, 6, 11, 14, 15, 16, 25, 29 and 30, and any provision intended by its nature to survive, survive termination.

22. Force majeure

22.1 Force majeure. Neither Party shall be liable for any failure, delay, interruption, suspension, inaccuracy or impaired performance of its obligations under these Terms to the extent caused by an event or circumstance beyond its reasonable control, including acts of God, natural disasters, flood, fire, epidemic, pandemic, war, terrorism, civil unrest, labour disputes, sanctions, governmental action, regulatory intervention, change in Applicable Law, utility failure, power outage, telecommunications or internet disruption, cyberattack, malicious code, denial-of-service event, blockchain congestion, consensus failure, chain reorganization, validator failure, hard fork, malfunction, smart-contract exploit, bridge failure, failure of a third-party provider or other comparable

event. The affected Party shall use reasonable efforts to mitigate the effects of the relevant event and resume performance as soon as reasonably practicable. Where reasonably practicable, the affected Party shall notify the other Party of the occurrence and general nature of the relevant event. If the relevant event continues for more than ninety (90) days and materially prevents performance of these Terms, either Party may terminate these Terms on written notice. Any such event affecting the DCV, a Strategy, an Approved Protocol or a material service dependency may also constitute a Suspension Event.

23. Notices

23.1 Form and permitted methods. Any notice, demand, request, consent, approval or other communication under or in connection with these Terms shall be in writing and shall be delivered by hand, by internationally recognized courier, by registered post with acknowledgement of receipt, or by email, in each case to the contact details most recently notified by the relevant Party and recorded in Annex A or through the Compliance App.

23.2 Deemed receipt. A notice shall be deemed received: (a) if delivered by hand, at the time of delivery; (b) if sent by courier or registered post, on the date shown in the delivery confirmation; and (c) if sent by email, at the time the email enters the recipient's information system, provided that no delivery-failure message is received by the sender. If deemed receipt would otherwise occur outside normal business hours at the place of receipt, the notice shall be deemed received at 9:00 a.m. on the next Business Day at that place.

23.3 Email notices. Notices sent by email satisfy any contractual requirement for writing under these Terms. The Parties acknowledge that operational communications, regulatory disclosures, material-event notices, statements, complaints responses, suitability reminders and durable-medium deliveries may validly be made by email and/or through the Compliance App or document drawer where these Terms so provide.

23.4 Contact details. Each Party shall keep its notice details current and shall notify the other Party promptly of any change. A notice sent to the last contact details notified in accordance with this clause shall be effective notwithstanding any internal failure by the receiving Party to forward or review it.

23.5 Excluded communications. This clause governs formal contractual notices and does not prevent the Parties from using the Compliance App, the Vault Interface, support channels or other agreed operational channels for day-to-day instructions, information requests, incident handling, onboarding steps or other operational matters, except where these Terms expressly require a formal notice.

24. Miscellaneous

24.1 Entire agreement. These Terms, together with the Annexes and the documents expressly incorporated by reference, constitute the entire agreement between the Parties in relation to their subject matter and supersede all prior discussions, negotiations, correspondence, representations, understandings and agreements relating to that subject matter.

24.2 No reliance on extraneous statements. Each Party acknowledges that, in entering into these Terms, it has not relied on any statement, representation, assurance or warranty other than those expressly set out in these Terms or in any mandatory pre-contractual information required by Applicable Law. Nothing in this clause limits or excludes liability for fraud or fraudulent misrepresentation.

24.3 Amendments. No amendment to these Terms shall be effective unless made in writing by or on behalf of both Parties, except where these Terms expressly permit an update, notification or operational amendment through a specified procedure, including in relation to Whitelisted Addresses, operational documents, protocol lists, product documentation or other items expressly identified as updateable under these Terms.

24.4 Waiver. No failure or delay by either Party in exercising any right, power or remedy under these Terms shall operate as a waiver of that right, power or remedy, nor shall any single or partial exercise preclude any other or further exercise of it or the exercise of any other right, power or remedy.

24.5 Severability. If any provision of these Terms is held to be illegal, invalid, void, unenforceable or ineffective in whole or in part under Applicable Law, that provision shall, to the extent required, be deemed severed and ineffective without affecting the legality, validity or enforceability of the remaining provisions. The Parties shall negotiate in good faith a valid replacement provision that most closely reflects the legal and commercial intent of the severed provision.

24.6 Assignment. Neither Party may assign, transfer, novate, charge, declare a trust over or otherwise dispose of any of its rights or obligations under these Terms without the prior written consent of the other Party, except that Tesseract may assign or transfer these Terms to an Affiliate or as part of a bona fide corporate reorganisation, merger, business transfer or financing transaction, provided that such assignment does not materially reduce the Client's substantive protections under these Terms.

24.7 No third-party rights. Except as expressly provided in these Terms, a person who is not a Party to these Terms has no right to enforce any term of these Terms.

24.8 Cumulative remedies. The rights and remedies provided in these Terms are cumulative and, except as expressly stated otherwise, do not exclude any rights or remedies provided by Applicable Law.

24.9 Further assurances. Each Party shall, at the reasonable request of the other Party, execute and do such further acts, documents and things as may reasonably be required to give full effect to these Terms and the transactions contemplated by them.

24.10 Costs. Unless expressly stated otherwise in these Terms, each Party bears its own costs of negotiating, preparing, entering into and performing these Terms.

25. Governing law and jurisdiction

These Terms are governed by and construed in accordance with the laws of Finland, without regard to conflict-of-laws principles. Any dispute, controversy or claim arising out of or relating to these Terms, including their validity, breach or termination, is submitted to the exclusive jurisdiction of the Helsinki District Court (Helsingin käräjäoikeus) as court of first instance, subject to any non-excludable right of the Client to bring proceedings elsewhere.

26. **Interpretation**

26.1 Interpretative safeguard. Nothing in these Terms, in any Strategy description, in any Product Information Summary, in any marketing communication or in any operational flow shall be interpreted as providing, promising or advertising interest or other remuneration by reason of the mere holding of an e-money token. Any return associated with a Vault is represented by Tesseract as deriving from active portfolio-management activity, deployment decisions and protocol participation carried out under the Investment Mandate and subject to the risks described in these Terms.

27. Client acknowledgements

27.1 The Client further acknowledges that: (a) blockchain transactions are generally irreversible once confirmed; (b) the availability, speed, finality and economics of on-chain actions depend on third-party networks and infrastructure outside Tesseract's control; (c) off-chain interfaces, dashboards, APIs and operational tools may be unavailable, delayed or incomplete from time to time without affecting the legal validity of on-chain states or of authenticated instructions otherwise validly submitted; and (d) Tesseract may rely on the records, logs, wallet interactions, confirmations and audit trails generated through the Compliance App, the Vault Interface and the relevant blockchain infrastructure, except to the extent manifest error is demonstrated.

28. Hard Forks and Airdrops

28.1 No obligation to support. Tesseract is under no obligation to support, claim, collect, retain or take any action in respect of any forked or airdropped asset, and may decline to do so where the asset is not a Supported Asset, is not on the Approved Protocols list, is a Restricted Asset under Annex D, or presents security, legal, AML or operational risk.

28.2 Handling and no guarantee. Where Tesseract is able and elects to support a forked or airdropped asset, it is handled in accordance with the Investment Mandate. Where it is not supported, Tesseract may, where technically feasible, return it to the Client's Whitelisted Address or take no action, and is not liable for any loss of value of, or inability to access, any unsupported forked or airdropped asset. The Client acknowledges that such assets may be of no value, untradeable or carry their own risks, and that Tesseract does not guarantee that any value will be realized from any Hard Fork or Airdrop.

28.3 Costs, timing and valuation. Tesseract shall have no obligation to incur any cost, expense, tax exposure, legal risk, technical burden or operational burden in connection with the support, claiming, segregation, valuation, safekeeping, transfer or liquidation of any forked or airdropped asset. Any action taken by Tesseract in relation to such asset may be subject to delay, technical limitation, market illiquidity, pricing uncertainty, custody constraints, compliance review and the availability of reasonable operational means. Tesseract gives no assurance that any forked or airdropped asset will have value, be transferable, be recoverable, be capable of liquidation, or be made available to the Client within any particular timeframe.

29. Legal process and competing claims

29.1 Legal process. If any attachment, garnishment, freezing or seizure order, levy, insolvency proceeding or other legal or regulatory process ("Legal Process") is asserted against the Client, a Vault or the Vault Assets,

Tesseract may (and where required by Applicable Law shall) suspend or restrict Deployment Actions, deposits, redemptions or transfers in respect of the affected Vault, including by activating the Guardian Pause (clause 6.2), until the Legal Process is satisfied, lifted or resolved.

29.2 Compliance. Tesseract may comply with any Legal Process or any order of a court or competent authority that it reasonably determines to be applicable, without first contesting it and without liability to the Client and will notify the Client where permitted by Applicable Law. Tesseract is not obliged to contest any Legal Process on the Client's behalf.

29.3 Competing claims. Where Tesseract receives competing or conflicting claims or instructions in respect of a Vault or the Vault Assets, it may decline to act (other than to safeguard the assets) until the competing claims are resolved by agreement of the claimants or by a final order of a competent court, and is not liable for declining to act in those circumstances.

29.4 Costs and non-custodial position. Reasonable costs and expenses Tesseract incurs in responding to a Legal Process or competing claim in respect of the Client may be recovered from the Client. For the avoidance of doubt, the non-custodial architecture means the Vault Assets remain the Client's on-chain at all times; nothing in this clause grants Tesseract any proprietary claim to the Vault Assets beyond the Fees due under clause 7.

29.5 Evidence and protective steps. Tesseract may require such evidence, documents, legal opinions, indemnities, undertakings or court orders as it reasonably considers necessary before acting in relation to any Legal Process, adverse claim, competing instruction or beneficial-ownership dispute. Pending satisfactory resolution, Tesseract may continue to safeguard the relevant assets, decline to process instructions, place the relevant Vault in a restricted state, or take other protective steps as it reasonably considers appropriate to preserve assets, maintain compliance and reduce exposure.

30. Platform access, security and intellectual property

30.1 Access and credentials. Access to the Compliance App, the Vault Interface and the Public API is through the authentication methods Tesseract makes available (including multi-factor authentication and, where applicable, third-party identity providers and wallet connection). The identifiers, passwords, confirmation codes, connected wallets and other elements used for access ("Access Credentials") are the Client's identifying information. For a Corporate Client, Access Credentials are made available to the Authorized Persons, and the Client is responsible for ensuring they are used only by and on behalf of the Client and its Authorized Persons.

30.2 Security and reliance. The Client is responsible for maintaining the security and confidentiality of its Access Credentials and connected wallets and for all activity conducted through them. Tesseract is entitled to rely on, and treat as duly authorized, any instruction authenticated through the Client's Access Credentials or Whitelisted Wallet. The Client shall notify Tesseract without undue delay of any known or suspected compromise. Consistent with clause 2.4, Tesseract is not responsible for loss arising from the Client's failure to safeguard its Access Credentials, compromise of the Client's own systems, or use of the Whitelisted Wallet's signing capability by any person the Client has permitted to access it.

30.3 Availability. Availability of the off-chain surfaces is as set out in Annex B; the on-chain components carry no availability commitment, and the Client retains the ability to read and operate the Vault directly through the Whitelisted Wallet using any Ethereum mainnet RPC.

30.4 Intellectual property. All intellectual property rights in the Compliance App, the Vault Interface, the Public API, Tesseract's smart-contract infrastructure, documentation and marks belong to Tesseract or its licensors. The Client is granted a non-exclusive, non-transferable, revocable right to use them solely to receive the services under these Terms, and shall not copy, reproduce, redistribute, reverse-engineer or create derivative works from them except as permitted by Applicable Law or with Tesseract's prior written consent. The Client shall not disclose to any third party any information made available through the platform that the Client should not have been able to access.

30.5 Acceptable use. The Client shall use the platform only for its proper purpose under these Terms and shall not interfere with, or attempt to circumvent, its security or integrity.

30.6 Suspension of access. Tesseract may suspend, limit or terminate access to the Compliance App, the Vault Interface, the Public API or any related feature where reasonably necessary for security, maintenance, incident response, legal compliance, sanctions, AML/CFT review, misuse prevention, protection of intellectual property, enforcement of these Terms or the protection of the Client, Tesseract or other users. Where reasonably practicable, Tesseract shall provide prior notice, however, prior notice is not required where immediate action is reasonably necessary.

30.7 Monitoring and records. Tesseract may monitor, log, record and analyse access, usage patterns, instructions, authentication events, wallet interactions, communications, device and browser data, and other relevant technical and operational information for security, fraud prevention, troubleshooting, auditability, service improvement, legal compliance and evidential purposes.

30.8 Restrictions. Except to the extent expressly permitted by Applicable Law, the Client shall not, and shall not permit any third party to: (a) scrape, harvest, index or systematically extract data from the platform; (b) circumvent access controls or security features; (c) use the platform for benchmarking, competitive analysis or the development of a competing product or service; (d) introduce malicious code or attempt to probe, scan or test the vulnerability of the platform; or (e) use the platform in a manner that is unlawful, abusive, misleading or likely to impair the platform or the rights of others.

31. Acceptance

31.1 Electronic acceptance. These Terms are accepted by an Authorized Person completing the acceptance step in the Compliance App at the end of the onboarding journey, together with confirmation of the Annex A particulars. A qualified or advanced electronic signature is not required to form a binding agreement between Tesseract and a Corporate Client; a click-through acceptance with the evidence in clause 31.2 is sufficient and binding under applicable law. Tesseract counter-accepts on completion.

31.2 Evidence. On acceptance, the audit log captures the version hash of the Terms and Annex A served, the timestamp, the IP address and user agent, and the identity of the accepting Authorized Person, on an append-only audit log retained for at least five years.

31.3 Durable medium. Tesseract delivers the accepted Terms and the populated Annex A to the Client on a durable medium (by email and in the in-app document drawer) immediately on counter-acceptance.

31.4 Evidential value. The Parties agree that electronic records, audit logs, version hashes, time stamps, delivery logs, access records, authentication events, IP logs, user-agent data, wallet interactions, blockchain records and other electronic evidence generated or retained in connection with the Compliance App, the Vault Interface, the document drawer or the relevant blockchain infrastructure shall be admissible in evidence and may be relied upon to the fullest extent permitted by Applicable Law for the purpose of proving the existence, content, acceptance, amendment, delivery, performance or breach of these Terms.

31.5 No invalidity by electronic form. The validity, enforceability, and binding effect of these Terms, any acceptance, any instruction, any notice, any acknowledgement, any disclosure, delivery, or any other communication under these Terms shall not be denied solely because it is in electronic form, is communicated through the Compliance App or another agreed electronic channel, or is evidenced by electronic records rather than wet-ink signature or paper originals.

31.6 Version control and precedence. The version of these Terms, Annexes and incorporated documents made available to and accepted by the Client through the Compliance App, as evidenced by the relevant version hash and audit records, shall be the authoritative version binding on the Parties, subject only to any later amendment validly made in accordance with these Terms.

Annexes

Annex A: Client particulars

Details in brackets below are captured via the SumSub compliance application form.

Client (contracting entity)	[legal name, registration number, jurisdiction]

Classification	Corporate Client
Client Type	[self-custody institutional / client using a Client's Custodian]
Authorized Persons	[primary; secondary; compliance contact; operations contact; legal-notice email]
Suitability outcome	Passed — access to all available Strategies (single aggregated DCV target market)
Vault(s) deployed	[populated per Vault Parameter Sheet — Supported Asset, Strategy, token symbol, addresses]
Fee schedule / overlay	Standard: 0.25% management; 30% performance (HWM); zero deposit/withdrawal. [per-Vault overlay, if any]
Whitelisted Address(es)	[address(es) registered on the Whitelisting Contract]
Custody arrangement	[self-custody/Client's Custodian/name of designated custody provider, or institutional Custodian]
Effective Date / version hash	[populated at acceptance]

Vault Parameter Sheets

Each Vault Parameter Sheet populates from the on-chain VaultDeployed event and the Client's elections through the Vault Interface; sheets are not separately signed. Standard fee schedule applies unless a per-Vault overlay is recorded. More detailed product information sheets can be found in the Vaults App product strategy drop down menu as downloadable pdfs.

Vault / Strategy	Asset / token	Withdrawal settlement	Status
USDC Conservative	USDC / teUSDC	T+1	Live
USDC Advanced	USDC / teUSDC-A	T+2 (target)	Available
wBTC Advanced	wBTC / tewBTC	T+2 (target)	Available
wETH Advanced	wETH / tewETH	T+2 (target)	Available

Annex B: Technical services and service commitments

- **1. Function of this Annex and relationship with the Terms**

1.1 Function and precedence. This Annex B sets out the technical and operational framework supporting the services under these Terms. It does not create or modify any substantive legal, regulatory, commercial or liability obligation except where these Terms expressly so provide. In the event of conflict between this Annex B and the body of these Terms, the body of these Terms shall prevail, except in relation to purely technical or implementation matters expressly addressed in this Annex B.

2. Technical service surfaces

2.1 Vault Interface. The Vault Interface comprises the Whitelisted Wallet interaction layer, the vault deployment flow, the vault smart-contract interaction layer, the withdrawal management flow and the whitelisting functionality, together with associated client-facing interfaces made available by Tesseract from time to time. The relevant smart-contract addresses and integration references are recorded in Annex E and/or the applicable technical documentation.

2.2 Compliance App. The Compliance App supports onboarding, KYB/KYC and related compliance workflows, the Article 81 MiCAR suitability process, contract-pack presentation and acceptance, durable-medium delivery, the document drawer, wallet-management functions, whitelisting-related workflows, Travel Rule and related compliance capture, and such further compliance or operational functionality as Tesseract may reasonably make available within the scope of the services.

- **2.3 Public API.** The Public API is a read-only interface through which Tesseract may make available operational and reporting data relating to vault discovery, decoded transaction history, performance time-series, strategy attribution, vault identification data and related information relevant to the Client's use of the services.

2.4 The technical service surfaces described in this Annex B are made available as operational channels supporting the services and do not limit the legal validity of on-chain states, authenticated instructions or other acts validly carried out under the Terms.

3. Technical documentation and implementation references

3.1 The canonical source for technical implementation details may be maintained by Tesseract in its then-current product or technical documentation, including API specifications, data formats, interface requirements, contract addresses, maintenance procedures, release processes, integration instructions and similar implementation materials.

3.2 For the avoidance of doubt, the technical documentation may clarify how a service is technically implemented, but shall not alter what Tesseract is contractually required to provide under the Terms.

3.3 If any technical documentation is updated in a manner that would reasonably require changes to the Client's systems, integrations or operational procedures, Tesseract shall provide reasonable notice through the Compliance App, email or another appropriate durable or operational medium, taking into account the nature and urgency of the change.

4. Availability, maintenance and continuity

4.1 The off-chain service surfaces made available by Tesseract, including the Compliance App, the document drawer and the Public API, shall be operated using commercially reasonable efforts and in accordance with the operational resilience, security and continuity framework maintained by Tesseract under Applicable Law, including where relevant DORA-related controls.

4.2 Tesseract may carry out scheduled or unscheduled maintenance, testing, patching, upgrades, security actions, remediation work or other operational interventions affecting the off-chain service surfaces where reasonably necessary for security, continuity, resilience, legal compliance, service integrity or performance.

4.3 Where reasonably practicable, Tesseract shall provide prior notice of scheduled maintenance or other planned operational interventions that are reasonably expected to materially affect the availability of the off-chain service surfaces.

4.4 The Client acknowledges that the on-chain elements of the DCV structure depend on third-party blockchain infrastructure and external protocol environments and do not carry a standalone availability commitment by Tesseract beyond the obligations expressly assumed in the Terms.

4.5 Subject to the technical design of the relevant vault and the rights and controls applicable under the Terms, the DCV structure is intended to preserve the Client's ability to verify relevant on-chain states independently through standard blockchain tools and infrastructure.

5. Support and incident handling

5.1 Tesseract shall maintain operational support channels for matters relating to onboarding, wallet and whitelisting workflows, contract-pack delivery, reporting access, document access, general service operation, technical incidents and other matters reasonably connected with the services.

5.2 Tesseract shall operate an internal incident-handling and escalation framework appropriate to the nature of the services, including classification, triage, escalation, remediation and communication procedures for technical, operational, compliance and security incidents.

5.3 Where an incident materially affects the Client's use of the services, the Client's vault operations, the Client's access to material service information, or the integrity or availability of relevant service surfaces, Tesseract shall notify the Client as soon as reasonably practicable through email, the Compliance App or another appropriate channel, subject to Applicable Law and the legitimate needs of incident containment, security and regulatory coordination.

5.4 Nothing in this Annex B limits any separate notification obligation expressly assumed by Tesseract elsewhere in the Terms, including in relation to Guardian Pause events, material events, complaints handling, reporting or regulatory disclosures.

6. Reporting and information access support

6.1 This Annex B supplements, and does not replace, the reporting and reconciliation obligations set out in clause 9 of the Terms.

6.2 Tesseract may provide the Client with access, through one or more technical service surfaces, to operational and reporting information relating to the Client's vaults, including transaction history, vault status, performance information, strategy data, fee information, wallet and whitelisting status, and related service information.

6.3 Any live, simulated, estimated or API-derived information made available through the Public API, dashboard or other technical service surface is provided as an operational information tool and shall be read together with the valuation, reporting and reconciliation framework set out in the Terms and, where applicable, Annex D.

7. Material-event and service communications

7.1 Tesseract may use the Compliance App, the document drawer, email and other agreed channels to communicate service notices, operational alerts, maintenance notices, material-event notifications, statements, reminders, contract-pack materials, disclosure updates and similar communications relevant to the services.

7.2 Where the Terms require delivery on a durable medium, Tesseract shall satisfy that requirement in the manner specified in the Terms. Where the Terms permit an operational communication channel, Tesseract may use the channel most appropriate to the nature of the communication.

- **8. Change management**

8.1 Tesseract may update the technical and operational aspects of the service surfaces, interfaces, integrations and supporting processes from time to time where reasonably necessary for security, resilience, legal compliance, product maintenance, operational efficiency or service improvement.

8.2 No update under this Annex B may, without compliance with the relevant contractual process under the Terms:

a) materially reduce the Client's contractual reporting rights;

b) materially reduce the Client's withdrawal or redemption rights;

c) materially reduce notification rights expressly granted in the Terms;

d) materially change the agreed allocation of liability, custody functions, fees or termination rights; or

e) materially alter the substantive characteristics of the services.

8.3 Where a change to a technical or operational matter would materially and adversely affect the Client's substantive position, Tesseract shall proceed in accordance with the relevant notice, amendment or termination provisions of the Terms.

9. Interpretation

9.1 This Annex B shall be interpreted consistently with:

a) the service description in clause 4;

b) the custody, ownership and control framework in clause 5;

c) the insolvency and wind-down framework in clause 6;

d) the reporting and reconciliation framework in clause 9; and

e) the notice, amendment and miscellaneous provisions of the Terms.

9.2 For the avoidance of doubt, this Annex B is not intended to create an independent or free-standing technology services agreement separate from the regulated and contractual service relationship established by the Terms.

Annex C: Risk disclosure

This risk disclosure is provided pursuant to Article 66 MiCAR. The Client should read it in full before accepting these Terms or depositing any crypto-assets.

1. Market and volatility risk

- **Price volatility:** crypto-assets are subject to extreme volatility; declines may be sudden and substantial and may result in total loss; markets operate 24/7 and significant moves may occur outside business hours.
- **Stablecoin de-peg:** strategies use e-money tokens (e.g. USDC) and other stablecoins which may de-peg temporarily or permanently on loss of reserves, issuer failure, loss of confidence, regulatory intervention or technical failure, potentially causing significant or total loss of the affected holdings; reserves are subject to the issuer's credit and investment risk, outside Tesseract's control.
- **Yield volatility:** DeFi yields are variable and may decline to zero or negative (where gas/protocol fees exceed returns); elevated yields may reflect higher risk; net yield differs from gross after fees and costs; no target or projected yield is guaranteed.
- **Foreign exchange risk**: where the Client's base currency differs from the asset denomination, FX fluctuations affect value; the DCV does not hedge currency.

- **Correlation and systemic risk:** crypto markets exhibit high correlation under stress; a systemic downturn may reduce all positions simultaneously; diversification does not eliminate systemic risk.
- **Passive breach:** market movements may cause the portfolio to deviate from Investment Mandate parameters without Tesseract action; Tesseract uses reasonable endeavors to restore compliance within 48 hours and is not liable for losses arising from a passive breach within that period.

2. DeFi protocol risk

- **Smart-contract vulnerabilities:** bugs, logic errors or design flaws may be exploited (reentrancy, flash-loan, overflow, access-control, economic-design), potentially causing partial or total loss; no audit guarantees the absence of vulnerabilities; assets lost before remediation may be irrecoverable.
- **Oracle risk**: smart contracts may rely on external data feeds; malfunction, manipulation or stale data may cause execution on incorrect inputs; Tesseract does not operate oracles and is not liable for oracle failure.
- **Composability/dependency risk:** interdependencies between protocols, oracles and bridges may cascade failures across the ecosystem even where the deployed protocol remains operational.
- **Liquidity and withdrawal risk:** withdrawals may be subject to queues, utilization constraints, lock-ups or insufficient liquidity; in extreme conditions withdrawal may not be possible or only at a significant discount; illiquidity is heightened during stress.
- **Leverage and liquidation risk:** certain Advanced strategies use on-chain leverage subject to liquidation where collateral falls below thresholds; rapid moves may prevent orderly deleveraging and cause cascading liquidations; leverage magnifies gains and losses and raises the risk of total loss.
- **Asset transformation / yield-bearing token risk:** deployment may wrap assets into yield-bearing equivalents; the Client retains beneficial ownership of the underlying, but the yield-bearing token carries additional peg and issuing-protocol risk.

3. Technology and infrastructure risk

- **Blockchain network risk:** congestion, consensus failures, reorganizations/forks, validator attacks (incl. 51%/MEV), base-layer bugs and hard forks.
- **Smart-contract infrastructure (IPOR Fusion):** the DCV uses the ERC-4626 standard and EIP-1167 minimal proxy on IPOR Fusion; these are relatively novel and may contain undiscovered vulnerabilities; an exploit in the underlying vault infrastructure could affect all DCVs; upgrades may introduce new risks.
- **Cybersecurity risk:** Tesseract, the sub-custodian and the DeFi protocols are targets for sophisticated attacks (phishing, DoS/DDoS, ransomware/supply-chain, front-end/DNS/BGP, insider threats); no system guarantees immunity; a successful attack could cause partial or total loss.
- **Private-key and wallet-security risk:** loss, theft or compromise of private keys may cause irreversible loss; blockchain transactions are generally irreversible; no key-management system eliminates all risk.

4. Custody and counterparty risk

- **Sub-custodian risk:** Where the Client uses a Client's Custodian or other third-party custody infrastructure, the Client bears residual risk relating to that provider's continuity, solvency, cybersecurity, operational resilience and regulatory standing. Prior to transfer into the DCV, relevant assets may be held through that custody infrastructure; once transferred into the DCV, they are held through the Client's individually segregated on-chain smart-contract vault. The applicable insolvency regime and protections may differ from those applying to Tesseract.
- **Counterparty risk in DeFi:** exposure to protocol and borrower counterparty risk; collateral may be insufficient in rapid declines, creating socialized bad debt; DeFi generally lacks deposit insurance, compensation schemes or central clearing; counterparties are typically pseudonymous.

5. Regulatory and legal risk

- **Evolving framework:** rapid, unpredictable regulatory change may restrict strategies/protocols, impose new requirements, reclassify the DCV/Vault Tokens/assets, require modification or termination, or create adverse tax consequences.
- **E-money token regulatory risk**: Article 50 MiCAR prohibits offering interest/yield on e-money tokens; Tesseract's position is that DCV yield derives from active deployment under a discretionary mandate,

not from holding an e-money token; a different regulatory interpretation could require restructuring or cessation of affected strategies.

- **Classification risk**: Tesseract's position is that the DCV is not a collective investment undertaking or AIF under AIFMD and that Vault Tokens are not transferable securities under MiFID II; a different conclusion could subject the DCV to additional requirements or require restructuring.
- **Tax and reporting (DAC8/CARF):** transaction data may be shared with tax authorities; the Client is solely responsible for its own tax obligations.
- **Cross-border risk:** cross-border provision may be subject to local licensing, marketing restrictions or prohibitions; the MiCA passporting framework's practical application may vary between Member States.

6. Operational risk

- **General operational/process risk**: failures of internal processes, systems, personnel or external providers may cause delays, errors or losses.
- **Key-person and continuity risk:** operations depend on a limited number of specialized personnel; departure or incapacity could impair management, strategy changes, incident response or compliance.
- **Guardian Pause:** a pause (triggered only by AML flags or regulatory instruction; market conditions excluded) may prevent access, withdrawal or rebalancing for an indeterminate period; Tesseract is not liable for losses arising from the activation or its timing; in wind-down the pause is lifted to permit direct on-chain redemption.
- **Third-party provider risk**: failure, insolvency or breach of a critical provider (sub-custodian, KYC/KYB, transaction-monitoring, smart-contract infrastructure, wallet connectivity) may impair the DCV; replacing a critical provider may cause disruption.

7. Insolvency and structural risk

- **Tesseract insolvency:** Client assets are held separately and do not form part of Tesseract's estate; recovery or return may nonetheless be delayed or challenged, particularly where assets are deployed or transformed.
- **Protocol insolvency/failure**: DeFi protocols generally lack legal personality; on critical failure, exploit or effective insolvency the Client may have no legal recourse and losses may be irrecoverable.
- **Sub-custodian insolvency:** Where the Client uses a Client's Custodian or other third-party custody infrastructure, assets held through that infrastructure prior to transfer into the DCV or after return from the DCV may be exposed to that provider's creditors depending on the applicable insolvency regime and legal characterization. Once transferred into the DCV, Vault Assets are held through the Client's individually segregated on-chain smart-contract vault. Outcomes cannot be guaranteed and may differ from those applying to Tesseract.

8. Extraordinary risk

- **Quantum computing**: future advances may render current cryptography vulnerable, potentially compromising blockchain security and private keys across the ecosystem; quantum-resistant solutions are in development with no assurance of timely implementation.

9. Risk of total loss

The Client acknowledges that, as a result of any one or more of the risks above (individually or in combination), the Client may suffer a total and irrecoverable loss of all crypto-assets deposited in the DCV; such loss may occur suddenly and without warning. Tesseract does not guarantee the return of any deposited assets, the payment of any yield, or the preservation of value. The Client should only deposit assets it can afford to lose in their entirety.

Annex D: Investment management mandate

1. Nature of the mandate

1.1 The Client grants Tesseract a discretionary investment management mandate within the meaning and scope contemplated by the Terms in relation to the Client's Vault Assets held through the Dedicated Client Vault structure.

1.2 The mandate is individual, non-pooled and vault-specific. Each DCV is established for a single Client and operates independently from any vault established for any other client. The mandate does not create a common fund, a pooled portfolio, a collective investment undertaking, or any arrangement under which the profits, losses, assets, liabilities or returns of one client are shared with or economically linked to those of another client.

1.3 The fact that Tesseract may:

- **a)** offer the same named Strategy to more than one client;
- **b)** use common strategy templates, protocol lists, allocation methodologies, monitoring tools, optimisation logic or execution procedures;
- **c)** maintain common governance, risk or approval processes across clients; or
- **d)** carry out technically similar or contemporaneous actions across multiple vaults, shall not of itself create pooling, commingling, collective portfolio management, a shared NAV, a shared economic exposure, or any economic linkage between clients.

1.4 Tesseract acts under this mandate within the strategy parameters, investment restrictions, operational safeguards, Approved Protocols framework, risk disclosures and client-specific settings applicable to the relevant Vault.

2. Scope of discretionary authority

2.1 Subject to the Terms, Tesseract may exercise discretion in relation to the relevant Vault in order to implement the applicable Strategy, including by:

a) deploying Vault Assets into Approved Protocols directly or through Tesseract-operated strategy infrastructure where permitted by the Terms;

b) withdrawing, rotating, reallocating, rebalancing or de-risking positions;

c) managing yield-bearing, wrapped, transformed or strategy-specific positions arising from deployment activity;

d) managing leverage, collateral, borrowings, hedging mechanics, liquidity buffers, health-factor thresholds or similar strategy tools where these form part of the applicable Strategy design;

e) taking operational actions reasonably incidental to the implementation, protection, monitoring, unwinding or orderly management of the relevant Strategy; and

f) taking such further actions as are expressly permitted by the Terms, this Annex D and the applicable Strategy documentation.

2.2 Tesseract's obligations under the mandate are obligations of skill, care, diligence and proper performance, and not obligations to achieve any specific investment outcome, yield level, liquidity profile or preservation of value.

- **2.3** The mandate shall be exercised consistently with the service description in clause 4, the asset-control and segregation principles in clause 5, the risk framework in the Terms, the conflicts framework, the suitability framework and the applicable product disclosures.

3. Acts excluded or requiring additional authority

3.1 Unless otherwise expressly permitted by the Terms, Tesseract shall not, under this mandate:

a) transfer Vault Assets to itself for proprietary purposes;

b) use Vault Assets for its own account or for the account of third parties otherwise than as strictly required for implementation of the agreed services and strategy mechanics;

c) deploy Vault Assets into any asset, protocol or strategy category prohibited by the Terms, the applicable Strategy constraints or any Client-specific restriction recorded for the relevant Vault;

d) create any pooling or commingling of the Client's assets with those of another client or with Tesseract's own assets;

e) assume any authority outside the scope of the services and operational architecture agreed in the Terms; or

f) take any action for which the Terms expressly require separate client consent, approval or instruction.

3.2 Any matter that would materially alter the agreed strategy envelope, the material risk profile, the liquidity profile, the nature of the exposure, or the substantive position of the Client shall be handled in accordance with the amendment, disclosure, notice or consent mechanics applicable under the Terms.

4. Strategy architecture and no collective effect

4.1 Each Vault runs a single Strategy selected within the framework described in the Terms. The Client's rights, exposure, performance, fees, withdrawal position and reporting remain attributable to that Client's own Vault.

4.2 Any use of model-driven execution, common strategy logic, standardised strategy schedules, protocol-eligibility lists, common operational infrastructure, batched or contemporaneous execution, or standardised risk controls are adopted for efficiency, consistency and risk management only and does not change the individual and segregated nature of the mandate.

4.3 Tesseract shall maintain the structural characteristics of the DCV model that support the individualised nature of the service, including segregated vault architecture, client-specific asset attribution, client-specific fee attribution, individual exit rights and the absence of any contractual sharing of investment performance across clients.

5. Approved Protocols and strategy governance

5.1 The protocols, infrastructure layers and deployment venues eligible for use within a Strategy shall form part of the Approved Protocols framework maintained by Tesseract in accordance with its internal governance, risk and compliance procedures.

5.2 Tesseract may add, remove, suspend, restrict or condition the use of an Approved Protocol or strategy component where reasonably required for security, legal, regulatory, liquidity, operational, technical, sanctions, AML/CFT, risk-management or resilience reasons.

5.3 A removal, suspension or restriction made in response to a security threat, protocol failure, regulatory issue, compliance concern or comparable risk event may take effect immediately where reasonably necessary to protect Vault Assets, maintain compliance or reduce risk.

5.4 Ordinary updates to the Approved Protocols framework that do not materially alter the substantive characteristics of the relevant Strategy may be made through the governance and update process described in the Terms and the relevant service documentation.

5.5 No update to the Approved Protocols framework may, without the contractual process required by the Terms, materially alter:

- **a)** the essential economic character of the relevant Strategy;
- **b)** the principal categories of risk assumed by the Client
- **c)** the expected liquidity profile in a materially adverse manner;
- **d)** the leverage profile or exposure architecture in a materially adverse manner; or
- **e)** the substantive rights or protections of the Client.

5.6 Where a proposed change would materially affect the Client's substantive position, Tesseract shall provide the disclosure, notice, amendment opportunity or termination right required by the Terms and Applicable Law.

6. Best execution, discretion and constraints

6.1 In exercising discretion under this mandate, Tesseract shall take all sufficient steps, in the context of the relevant crypto-asset service, to obtain the best possible result for the Client having regard to the characteristics of the relevant Strategy and the operational environment in which it is executed.

6.2 In the DCV and DeFi context, the best possible result may take into account, where relevant:

- **a)** expected net outcome after fees, slippage, protocol costs and transaction costs;
- **b)** available on-chain or protocol liquidity;
- **c)** likelihood and speed of execution, settlement, withdrawal or unwind;
- **d)** smart-contract, protocol, oracle, bridge, custody-layer and blockchain risk;
- **e)** collateral, leverage and liquidation constraints;
- **f)** operational resilience, market conditions and risk-reduction considerations; and
- **g)** any legal, regulatory, sanctions, AML/CFT or technical restriction affecting execution.

6.3 The Client acknowledges that in certain market or protocol conditions, the best possible result may reasonably require Tesseract to prioritise risk reduction, orderly execution, liquidity preservation, compliance, or asset protection over immediate price or yield optimisation.

7. Valuation, monitoring and operational implementation

7.1 Tesseract may use on-chain data, oracle data, protocol data, internal calculation tools, operational dashboards, API infrastructure and related systems to monitor and manage the relevant Vault.

7.2 Any valuation, NAV, vault-token-price, monitoring or strategy-analytics methodology used in connection with the mandate shall be applied consistently with the valuation, reporting and reconciliation framework set out in the Terms.

7.3 Where different information surfaces provide real-time, on-touch, estimated or statement-based information, they shall be interpreted according to their function under the Terms, and no operational data surface shall of itself displace the contractual reporting framework.

8. Client-specific parameters and restrictions

8.1 Tesseract may apply standard strategy parameters, risk controls, concentration limits, collateral thresholds, liquidity rules, de-risking mechanics, operational constraints and similar controls to the relevant Strategy.

8.2 Any Client-specific restriction, tighter limit, prohibited exposure, operational constraint or other bespoke parameter expressly accepted by Tesseract for the relevant Vault shall prevail over the default strategy parameter to the extent of the inconsistency.

8.3 Tesseract may rely on the Client particulars, suitability information, eligibility status, wallet configuration and other operational information recorded for the relevant Vault when implementing the mandate.

9. Breach, deviation and remediation

9.1 A deviation caused solely by market movement, protocol conditions, valuation changes, liquidity shifts, oracle movement, automated deleveraging conditions or other factors not involving a deliberate deployment action by Tesseract shall not, of itself, constitute a breach of mandate if Tesseract acts within a reasonable period and in a manner consistent with the Terms to assess, manage, reduce or remediate the deviation.

9.2 A deliberate action by Tesseract that falls outside the mandate, the applicable restrictions or the agreed strategy parameters shall be treated in accordance with the liability, notification and remediation framework set out in the Terms.

9.3 Where reasonably required, Tesseract may take protective or de-risking steps on an interim basis pending full remediation, including pausing, reducing exposure, unwinding positions, restricting deployment activity or taking other actions reasonably connected with asset protection, compliance or orderly risk management.

9.4 Upon becoming aware of any breach of the Investment Mandate, whether active (caused by a deliberate Deployment Action) or passive (caused by market movement, oracle shift, or other involuntary factor), the Company shall:

(a) notify the Client in writing within one (1) Business Day, identifying the parameter affected, the cause, the magnitude, and proposed remediation steps; and

(b) confirm remediation in writing promptly upon restoration of compliance, and in any event within five (5) Business Days of the breach notification in the case of an active breach.

10. Relationship with other contractual documents

10.1 This Annex D shall be interpreted together with:

- **a)** clause 3 (Suitability assessment);
- **b)** clause 4 (Appointment, scope of services, Vaults and Strategies);
- **c)** clause 5 (Custody, ownership and asset control);
- **d)** clause 6 (Insolvency protections);
- **e)** clause 9 (Reporting and reconciliation);
- **f)** clause 13 (Risk allocation);
- **g)** clause 17 (Conflicts of interest);
- **h)** Annex C (Risk disclosure); and
- **i)** the relevant Strategy schedules and product disclosures.

10.2 In the event of conflict or inconsistency between this Annex D and the body of the Terms, the body of the Terms shall prevail on any legal, regulatory, commercial, liability, disclosure, custody, client-rights or other substantive matter, and this Annex D shall prevail only in relation to the detailed operational implementation of the mandate to the extent consistent with the Terms.

10.3 For the avoidance of doubt, this Annex D does not create any fiduciary, depositary, trustee, pooling, collective-investment or other legal relationship beyond the regulated and contractual relationship expressly set out in the Terms.

Annex E: Strategy Schedules

All four Strategies sit within the same MiCAR high-risk suitability band and a single aggregated DCV target market. A Client who has passed the suitability assessment may deploy any and all of them, across one or more Vaults, and may open and close Vaults freely (clause 4.5).

Each Strategy is pre-drafted and RCC-approved before going live for Client deployment, and is accompanied by a Product Information Summary which is provided to the Client before deployment via the Vault app and forms part of the information on which suitability and deployment are based. The Product Information Summary for each Strategy is the source document for that Strategy's indicative target return (quoted gross), strategy mechanics, risk profile and

Strategy A — USDC Conservative

Product type	Lending Optimizer Vault
Supported Asset / exposure	USDC (USD Coin)
Risk classification	Conservative (within the single aggregated DCV target market)
Indicative target return	~5–6% (Gross); indicative, not guaranteed — see the Product Information Summary
Yield mechanism and parameters	Rules-based lending optimizer allocating USDC across approved DeFi lending markets (e.g. Aave, Morpho, Euler, Fluid). No leverage, looping, derivatives or LP exposure outside the approved list; capital preservation prioritized; concentration limits per protocol; liquidity reserve to support redemption within the liquid balance.
Approved Protocols	Per the Strategy Schedule and the IPOR Fusion deployment; the protocol list is maintained and updated by RCC resolution (Annex D).
Strategy-specific risk highlights	Smart-contract risk in lending protocols; stablecoin issuer / de-peg risk; oracle risk; protocol governance risk; liquidity risk under stress.
Product Information Summary	The source document for this Strategy (overview, indicative target return (gross), strategy mechanics, risk profile, costs and fees, liquidity and key risks), provided as pre-contractual disclosure, see Clause 1.3.

Strategy B — USDC Advanced

Product type	Leveraged Carry / Looping
Supported Asset / exposure	USDC (USD Coin)
Risk classification	Advanced / Higher Risk (within the single aggregated DCV target market)
Indicative target return	~7–10% (Gross); indicative, not guaranteed — see the Product Information Summary
Yield mechanism and parameters	Converts USDC into yield-bearing stablecoin assets supplied as collateral on approved lending platforms, borrows USDC and loops to enhance capital efficiency and yield, with incentive-driven lending. Leveraged positions are managed to a strategy-specific target Health Factor (not a fixed leverage cap), actively monitored and adjusted.
Approved Protocols	Per the Strategy Schedule and the IPOR Fusion deployment; the protocol list is maintained and updated by RCC resolution (Annex D).
Strategy-specific risk highlights	Liquidation risk (positions managed to a target Health Factor); smart-contract risk including in leveraged positions; oracle risk; IPOR Fusion dependency; stablecoin peg / counterparty risk; incentive volatility; correlation risk under stress.
Product Information Summary	The source document for this Strategy (overview, indicative target return (gross), strategy mechanics, risk profile, costs and fees, liquidity and key risks); provided as pre-contractual disclosure — see Clause 1.3.

Strategy C — wBTC Advanced

Product type	Carry / Leveraged Staking
Supported Asset / exposure	Bitcoin (via wBTC)
Risk classification	Advanced / Higher Risk (within the single aggregated DCV target market)
Indicative target return	~1–3% (Gross); indicative, not guaranteed — see the Product Information Summary
Yield mechanism and parameters	Supplies wBTC as collateral across approved lending markets, borrows (typically stablecoins) and redeploys into yield-generating carry strategies; the Vault accepts wBTC deposits and yield is denominated in wBTC. Leveraged positions are managed to a strategy-specific target Health Factor (not a fixed leverage cap), actively monitored and adjusted.
Approved Protocols	Per the Strategy Schedule and the IPOR Fusion deployment; the protocol list is maintained and updated by RCC resolution (Annex D).
Strategy-specific risk highlights	Liquidation risk (positions managed to a target Health Factor); BTC price volatility; smart-contract risk; stablecoin / counterparty risk; incentive volatility.
Product Information Summary	The source document for this Strategy (overview, indicative target return (gross), strategy mechanics, risk profile, costs and fees, liquidity and key risks); provided as pre-contractual disclosure — see Clause 1.3 .

Strategy D — wETH Advanced

Product type	Leveraged Staking and Yield Strategy
Supported Asset / exposure	Ethereum (wETH)
Risk classification	Moderate / High (within the single aggregated DCV target market)

Indicative target return	~2–4% (Gross); indicative, not guaranteed — see the Product Information Summary
Yield mechanism and parameters	Converts wETH into liquid staking derivatives (e.g. stETH, wstETH) supplied as collateral, borrows and redeploys into additional yield strategies, combining staking yield with DeFi carry; the Vault accepts wETH deposits and yield is denominated in wETH. Leveraged positions are managed to a strategy-specific target Health Factor (not a fixed leverage cap), actively monitored and adjusted.
Approved Protocols	Per the Strategy Schedule and the IPOR Fusion deployment; the protocol list is maintained and updated by RCC resolution (Schedule D).
Strategy-specific risk highlights	Liquidation risk (positions managed to a target Health Factor); ETH price volatility; liquid-staking-derivative de-peg risk (stETH / wstETH); smart-contract risk; incentive volatility.
Product Information Summary	The source document for this Strategy (overview, indicative target return (gross), strategy mechanics, risk profile, costs and fees, liquidity and key risks); provided as pre-contractual disclosure — see Clause 1.3.

Cross-strategy items (all four)

- **Fees:** The fees applicable to each Strategy are set out in clause 7 and Annex A, unless varied by a per-Vault overlay recorded in the relevant Vault Parameter Sheet.
- **NAV and valuation**: NAV, Vault Token Price, valuation methodology and periodic reporting apply in accordance with clause 9 and Annex D.
- **Rebalancing and de-risking:** Rebalancing, de-risking measures and protocol-level risk controls are applied by Tesseract in accordance with these Terms, Annex D and the applicable operational procedures.
- **Suitability:** All Strategies fall within the same aggregated DCV target market. A Client who has passed the suitability assessment may deploy any available Strategy, subject to these Terms.
- **Governance:** Each Strategy is subject to Tesseract's internal approval and governance process, including approval of material strategy parameters and protocol eligibility.
- **Custody:** across all Strategies, the DCV structure operates within a MiCAR-regulated custody-and-administration framework combined with a layered operational custody architecture. Vault Assets remain on-chain or within the relevant custody-wallet layer, beneficial ownership remains with the Client at all times, private keys remain under the control of the Client or its third-party custody provider, and Tesseract does not hold the Client’s private keys or acquire any proprietary interest in Vault Assets by reason only of the services performed under these Terms