5) On-Chain Permission Policy

Version: V001.005.015
Last updated: Tuesday, 10 February 2026
Effective date: Friday, 30 January 2026
Issuer: FUSAUSD Financial Ltd. (the "Issuer")
Principal place of business: Wigmore Street, Marylebone, London W1U 3RY, United Kingdom

This On-Chain Permission Policy (this "Policy") describes the design, allocation, and operation of administrative permissions for the FUSAUSD Stablecoin smart contracts (the "Contracts") on each Supported Network. This Policy forms part of the FUSAUSD Stablecoin program documentation and must be read together with the Terms of Issuance & Redemption, the Reserve Policy, the Transparency Policy, and the Operational Controls (collectively, the "Program Documents"). If this Policy conflicts with the Terms of Issuance & Redemption, the Terms of Issuance & Redemption control.

5.1 Contract architecture

5.1.1 The FUSAUSD Stablecoin is implemented as a standards-based token contract on each Supported Network. On EVM-compatible networks, the primary token interface follows the ERC-20 standard. Optional features (if any), such as EIP-2612 "permit" approvals or transfer-by-signature, are listed per network in Schedule 5-B.

5.1.2 The Issuer maintains a canonical registry of Supported Networks and Contract Addresses (the "Registry"). The Registry is published and versioned. Any addition, deprecation, or replacement of a Contract Address is treated as a material change and disclosed in accordance with the Transparency Policy.

5.1.3 The Contracts are deployed using either (a) an immutable implementation with no upgrade function, or (b) an upgradeable architecture using a proxy pattern. The architecture choice for each Supported Network is stated in Schedule 5-A. Where upgradeability is used, the Issuer separates proxy administration from routine operational roles and uses time-delay controls for upgrades as described in Section 5.5.

5.1.4 Where practicable, critical functionality is separated into modules: (i) token logic (balances and transfers), (ii) issuance and redemption controls (mint and burn), (iii) compliance controls (blocking, freezing, wiping), and (iv) administrative governance (role assignment and upgrades). Module separation is intended to support least-privilege access and to reduce the blast radius of any single permission.

5.1.5 Administrative functions are restricted to explicit Roles (defined below) and are callable only by addresses recorded in the on-chain access control state. No administrative function is intended to be callable by a tokenholder except where expressly stated in the Program Documents (for example, a user-initiated burn path, if offered).

5.1.6 Each Supported Network has a defined "finality rule" for authoritative state, including for reporting snapshots and for determining when an on-chain administrative action is treated as effective for operational purposes. The finality rule per Supported Network is set out in Schedule 5-C.

5.1.7 On-chain permissions are administered on a per-network basis. A permission on one Supported Network does not imply any permission on any other Supported Network, except to the extent the Issuer expressly discloses a shared control plane (for example, a common multisig used across networks).

5.1.8 Cross-chain wrappers, bridges, and third-party representations of the FUSAUSD Stablecoin (including "bridged" or "wrapped" tokens) are not "Contracts" unless the Issuer expressly designates them as such in the Registry. The Issuer may treat third-party wrappers as unsupported, even where they exist on public networks.

5.1.9 Where the Issuer supports a non-EVM network, the Issuer describes in Schedule 5-A the equivalent permission model (including upgrade authority, pause capability, and compliance controls) and the method by which administrative actions are logged and verified on that network.

5.2 Roles and authorities

5.2.1 **Role taxonomy.** The Contracts may implement a role-based access control system. The Issuer publishes the role taxonomy, including function scope for each role, in Schedule 5-B, and labels controlling addresses in the Registry described in Section 5.4.

5.2.2 **Governance Role.** The "Governance Role" is the ultimate administrative authority for (i) granting and revoking Roles, (ii) changing sensitive configuration parameters (including mint limits), and (iii) authorizing upgrades where upgradeability exists. The Governance Role is held through a multisignature wallet or institutional custody arrangement that meets Section 5.3.

5.2.3 **Minter Role.** The "Minter Role" may invoke minting functions subject to allowlists, amount limits, and workflow constraints. Minting is permitted only in connection with issuance under the Terms of Issuance & Redemption and only after the Issuer's settlement and compliance conditions have been satisfied.

5.2.4 **Minter limits and throttles.** Where supported, the Contracts enforce per-minter limits, aggregate daily caps, and other throttles designed to bound operational error and reduce the impact of compromised credentials. Limit changes are treated as controlled administrative actions and are logged.

5.2.5 **Burner Role.** The "Burner Role" may burn tokens held by Issuer-controlled wallets in connection with redemption, treasury operations, and error correction. Burning destroys tokens on-chain; it does not itself move fiat and does not replace the redemption process described in the Terms of Issuance & Redemption.

5.2.6 **User-initiated burn (optional).** The Issuer may offer a user-initiated burn function, for example to allow a tokenholder to destroy tokens without requesting fiat redemption. If offered, the feature and its effects (including whether any redemption right attaches) are described in the Terms of Issuance & Redemption and reflected in Schedule 5-B.

5.2.7 **Pause Role.** The "Pause Role" may invoke a pause function that restricts some or all token operations. The scope of pausing (for example, transfers only; mint/burn only; or all functions) is defined per network in Schedule 5-B.

5.2.8 **Permitted pause triggers.** Pausing is permitted only where reasonably necessary to address (i) a credible security incident, (ii) a material smart contract vulnerability or exploit, (iii) a

Supported Network outage, reorganization, or consensus failure, (iv) a material disruption to reserve custody or settlement that threatens orderly redemption processing, or (v) a legal or regulatory requirement. Pausing decisions follow the incident response playbook in the Operational Controls and are documented.

5.2.9 **Compliance Role (Blocklist/Freeze).** The "Compliance Role" may designate an address as blocked or restricted (a "Blocked Address") such that the Contracts prevent transfers to or from that address. Blocking or freezing is used to comply with applicable law, sanctions, court orders, or documented internal compliance determinations consistent with the Program Documents.

5.2.10 **Effect of blocking.** Where blocking is applied, the affected address may be prevented from sending and/or receiving the Stablecoin on that Supported Network. The Contracts may also restrict minting to or burning from a Blocked Address. The specific restrictions are described per network in Schedule 5-B.

5.2.11 **Notice and administrative review.** Where permitted by law and operationally feasible, the Issuer may provide notice to an affected account holder through program channels. The Issuer may provide an administrative review mechanism; however, the Issuer may act without advance notice where required by law or where providing notice would reasonably increase risk of loss, evasion, or non-compliance.

5.2.12 **Unblock/Unfreeze.** Unblocking requires documented compliance review and is executed only by the Compliance Role (or a higher authority role), subject to the multi-party controls and logging requirements of Section 5.3. The Issuer maintains records of unblock determinations.

5.2.13 **Wipe / forced burn authority.** If implemented, the Contracts may include a function that allows the Issuer to irreversibly destroy tokens held by a Blocked Address ("Wipe"). Wipe is an extraordinary control and may be used only where (i) required by applicable law or binding legal directive, (ii) necessary to effect lawful seizure, forfeiture, or recovery processes, or (iii) necessary to remediate a critical technical incident where tokens are provably unrecoverable or where continued circulation would materially increase user harm.

5.2.14 **Controls for Wipe.** A Wipe action requires (i) Compliance Role approval, (ii) Security Role confirmation of the target address and amount, and (iii) Governance Role execution (or Governance Role co-signature) unless emergency procedures in Section 5.3.9 apply. Where practicable, the Issuer links the action to a legal directive or incident reference.

5.2.15 **Reissue after Wipe.** The Issuer is not obligated to reissue tokens after a Wipe. If the Issuer elects to reissue, it does so only to an address that has completed required compliance checks and only where legally permitted. Any reissue is treated as a mint and remains subject to this Policy and the Terms of Issuance & Redemption.

5.2.16 **Role assignment and delegation.** Role assignment, revocation, and sensitive configuration changes (including minter limits and compliance configuration) are administrative actions requiring the Governance Role. The Issuer may delegate limited operational roles to regulated service providers (for example, an institutional custodian operating a signing service) provided the delegation is disclosed, contractually controlled, and revocable.

5.3 Key management

5.3.1 **General standard.** Administrative permissions are exercised only through key management procedures designed to prevent unauthorized use, reduce single-person control, evidence all actions, and support rapid response to compromise.

5.3.2 **Multisignature requirement.** The Governance Role and any role capable of (i) upgrading Contracts, (ii) changing Roles, (iii) changing mint limits, or (iv) performing a Wipe must be implemented as a multisignature arrangement (M-of-N). Minimum thresholds by role are specified in Schedule 5-D. Single-signature administrative keys are not permitted for those functions.

5.3.3 **Signer independence.** Signers must be organizationally independent. At least one signer must be from each of the following functions: security, compliance/legal, and treasury/finance. No signer may approve an administrative action that they originated without an additional independent signer.

5.3.4 **Key custody.** Private keys for administrative roles are stored using hardware-backed key custody controls, including HSM-backed signing, institutional custody with dual control, or equivalent secure enclaves. Keys must not be stored in plaintext on general-purpose devices. Backup material is stored under a documented secure storage process and is accessible only under dual control.

5.3.5 **Access reviews.** The Issuer performs periodic access reviews for all on-chain administrative Roles, at least quarterly and upon relevant personnel changes. Reviews confirm signer identity, role necessity, and the continued validity of contact and escalation paths.

5.3.6 **Rotation.** Administrative keys are rotated (i) on a fixed cadence set out in Schedule 5-D, (ii) upon any compromise suspicion, (iii) upon signer departure or role change, and (iv) after material incidents. Rotation includes revocation of prior keys and verification of custody controls for replacement keys.

5.3.7 **Change management.** Changes to on-chain permissions are executed through a controlled change process: a written change request, risk review, independent approval, execution with the required signer threshold, and post-change verification on-chain. Emergency changes follow Section 5.3.9.

5.3.8 **Transaction construction and verification.** For each administrative transaction, the Issuer requires: (i) a prepared transaction payload created by an operator, (ii) independent verification of the target network, contract address, function selector, parameters, and expected events, and (iii) signer review of a human-readable summary and raw call data. The Issuer retains signed transaction data, the confirmed transaction hash, and verification evidence.

5.3.9 **Emergency procedures.** In emergencies (including suspected key compromise or active exploit), the Issuer may execute emergency pause or emergency role rotation procedures. Emergency procedures may temporarily reduce operational delays but may not reduce signer thresholds below the minimum set in Schedule 5-D. The Issuer documents the emergency basis, actions taken, and restoration steps, and discloses material events under the Transparency Policy.

5.3.10 **Separation from reserve custody.** Keys controlling reserve assets (banking and custody accounts) are separate from keys controlling on-chain administrative permissions. No single control plane is permitted to move reserve assets and also mint the Stablecoin without independent approvals and recordkeeping.

5.3.11 **Third-party signing services.** Where a third-party signing service is used, the Issuer requires: (i) contractual SLAs, (ii) incident notification obligations, (iii) audit and attestation rights, (iv) documented subprocessor controls, and (v) the ability to migrate to an alternate provider. The Issuer retains the ability to revoke the service's signing authority.

5.3.12 **Record retention.** The Issuer retains key management records, access reviews, change tickets, signer approvals, incident documentation, and supporting evidence for at least the retention period specified in Schedule 5-E or as required by applicable law.

5.4 Transparency by design

5.4.1 **On-chain events.** The Contracts emit on-chain events for administrative actions, including mint, burn, role grants/revocations, pause/unpause, block/unblock, and Wipe (if implemented). The event list per Supported Network is set out in Schedule 5-B.

5.4.2 **Public registry.** The Issuer publishes a labeled Registry identifying (i) each Supported Network, (ii) the Contract Addresses, and (iii) the administrative addresses controlling key Roles, including Governance, Minter, Pause, and Compliance Roles. The Issuer updates the Registry promptly after any change.

5.4.3 **Timelock visibility.** Where a timelock is used for upgrades or sensitive configuration changes, the timelock contract address, the delay duration, and queued operations are publicly observable. The Issuer discloses timelock parameters and any emergency bypass mechanism (if any) in Schedule 5-A.

5.4.4 **Disclosure of material changes.** The Issuer discloses material changes to on-chain permissions, including upgrades, changes to Governance Role addresses, changes to Compliance Role addresses, and changes to mint limits that materially affect risk. Disclosures follow the timelines and channels in the Transparency Policy.

5.4.5 **Administrative activity reporting.** The Issuer may publish periodic summaries of administrative actions, including mints and burns (counts and amounts), the number of block/unblock actions, and any Wipe actions, in a format reasonably capable of reconciliation to on-chain events and internal records.

5.4.6 **Event consumption and integrity.** For reporting purposes, the Issuer treats on-chain events as the primary public evidence of administrative actions, subject to the finality rules in Schedule 5-C. The Issuer maintains indexers and verification checks to detect missed events, chain reorganizations, and duplicate processing.

5.4.7 **Public audit trail.** Where supported by the network, sensitive changes (such as role changes and mint limit changes) are configured to emit explicit events, and the Issuer avoids "silent" configuration changes. The Issuer retains internal approval records that can be matched to the corresponding on-chain transaction hashes.

5.4.8 **Legal limitations.** The Issuer may be restricted by law from providing advance notice of enforcement actions or from disclosing certain details. The Issuer's transparency commitments are subject to applicable legal constraints.

5.5 Security

5.5.1 **Pre-deployment audit.** Before deploying Contracts on a Supported Network, the Issuer obtains an independent smart contract security review. For major deployments or upgrades, the Issuer targets at least two independent reviews, or one review plus formal verification, depending on scope and risk.

5.5.2 **Upgrade discipline.** Where upgradeable Contracts exist, upgrades are limited to clearly defined purposes (bug fix, security patch, standards support, or compliance necessity), are subject to timelock delays where feasible, and are executed only after testing and review. Emergency upgrades may be executed more quickly only where needed to prevent loss or systemic failure and remain subject to Section 5.3.9.

5.5.3 **Least privilege.** Roles are designed to minimize authority. Routine operational roles (minter/burner) are separate from Governance and Compliance Roles. No routine role includes the ability to both change permissions and execute high-impact functions without Governance Role involvement.

5.5.4 **Monitoring and alerts.** The Issuer implements monitoring for (i) unusual mint or burn activity, (ii) administrative function calls, (iii) abnormal transaction patterns suggestive of compromise, and (iv) Supported Network anomalies (including reorgs and halts). Alerts are integrated with the incident response playbook and communication plan in the Operational Controls.

5.5.5 **Bug bounty and responsible disclosure.** The Issuer maintains a responsible disclosure channel for security reports and may operate a bug bounty program. Reports are triaged under defined timelines and handled under confidentiality controls until remediation is deployed.

5.5.6 **Secure development and release controls.** Contract source code, deployment scripts, and configuration are maintained under version control with protected branches, code review requirements, and signed release artifacts. Deployment and upgrade runs use checklists that include verification of bytecode, role assignments, and expected events.

5.5.7 **Network and contract risk.** Each Supported Network introduces consensus and finality risks that may affect the Contracts. The Issuer evaluates network risks as part of Supported Network approval and discloses known unresolved events or occurrences that materially affect token operations, including smart contract or network issues, in accordance with the Transparency Policy.

5.5.8 **Forks and migrations.** In the event of a chain fork or migration, the Issuer may designate the canonical chain for program purposes. The Issuer may pause minting and redemption operations during an assessment period. The determination of canonical chain and any migration steps are communicated to users as soon as practicable.

5.5.9 **Drills and readiness.** The Issuer conducts periodic tabletop or simulation exercises covering key compromise, emergency pause, and recovery of administrative control. Exercises are documented and used to improve playbooks and signer readiness.

5.5.10 **Business continuity.** The Issuer maintains a tested ability to execute critical administrative actions (pause, revoke roles, rotate keys) during partial infrastructure failures, using out-of-band communication channels and pre-established signer contact paths.

5.5.11 **Third-party assurance.** Where feasible, the Issuer aligns smart-contract operations with external assurance expectations for stablecoin operations controls (for example, control objectives covering change management, access controls, and incident response) and obtains appropriate third-party reporting on those controls.

Schedules

Schedule 5-A (Contracts and architecture): Contract Addresses per Supported Network; proxy vs immutable; timelock address and delay; upgrade authority address.
Schedule 5-B (Role and function matrix): roles present; controlling addresses; function scope; event list; optional features (permit/signature transfers).
Schedule 5-C (Finality rules): per Supported Network finality rule used for authoritative state and reporting snapshots.
Schedule 5-D (Key management parameters): signer count and thresholds by role; signer independence requirements; rotation cadence; emergency procedures.
Schedule 5-E (Records retention): minimum retention period and evidence artifacts.