MONEYSAFE WALLET · MONEYSAFEWALLET.COM

Partner Admission Policy

Governance, due diligence, onboarding, monitoring and enforcement

Policy owner: MoneySafe

Jurisdictional focus: Greece and the European Union

Version: 2.0

Policy approver: Director / Compliance Committee

Effective date: 28 September 2026

Review frequency: At least annually and before any material programme or network change

Contents

1. Policy purpose
2. Policy statement
3. Scope and related documents
4. Definitions
5. Governance and accountability
6. Admission lifecycle and approval gates
7. Eligibility and due diligence
8. Risk classification
9. Approval authority and decision matrix
10. Permitted jurisdictions
11. Product and service categories
12. Technical onboarding and whitelisting
13. Contractual minimum requirements
14. Monitoring and audit
15. Suspension, reinstatement and removal
16. Partner Register and records
17. Exceptions
18. Reporting and escalation
19. Admission and activation checklist

---

1. Policy purpose

This Policy establishes the mandatory requirements for admitting, onboarding, activating, monitoring, restricting, suspending and removing partners from the MoneySafe Wallet Rewards Programme.

It is designed to ensure that:

- only suitable and adequately verified businesses participate;
- the partner network remains controlled and genuinely limited;
- participating partners offer lawful and approved products or services;
- MoneySafe identifies and manages legal, regulatory, financial-crime, consumer, fraud, technology and reputational risks;
- partner redemptions can be verified, reconciled and audited;
- customers receive the benefits advertised to them; and
- MoneySafe can take prompt corrective action where a partner creates risk or fails to meet its obligations.

No business may participate in the MoneySafe Wallet Rewards Programme unless it has completed the admission and activation process in this Policy.

2. Policy statement

MoneySafe will apply a documented, risk-based and evidence-led admission process to every Applicant.

Approval is conditional and may be withdrawn. An Approved Partner must remain within its approved legal entity, jurisdiction, product or service category, offer scope, technical configuration and settlement arrangements.

The partner network must remain controlled in:

- participating entities;
- jurisdictions;
- product and service categories;
- customer-facing offers;
- technical access;
- redemption functionality; and
- settlement arrangements.

This control framework supports the intended closed-loop character of the MoneySafe Wallet Rewards Programme. It does not, by itself, determine the programme's regulatory classification.

3. Scope and related documents

This Policy applies to all merchants, service providers, venues, professional businesses, online businesses, platforms and other entities seeking to participate in the MoneySafe Wallet Rewards Programme.

It should be read together with:

- the MoneySafe Wallet Rewards Programme Policy;
- the Partner Agreement;

- the Rewards Programme Rules;
- the Customer Terms;
- the Privacy Policy;
- the Information Security Policy;
- the Incident Response Policy; and
- the applicable refund, chargeback and complaints procedures.

Where documents conflict, mandatory law prevails. The signed Partner Agreement governs the commercial relationship. Any conflict that could affect the controlled or limited nature of the network must be escalated to the Policy Owner and Legal/Compliance before activation or continuation.

---

4. Definitions

Applicant

A business or organisation seeking admission.

Approved Partner

An Applicant that has completed the required review, received the required approval, signed the Partner Agreement and been technically activated.

Eligible Offer

A discount or promotional benefit approved by MoneySafe and displayed or communicated through authorised channels.

Eligible Redemption

A customer redemption that satisfies the applicable offer conditions and the technical and evidential requirements of the Partner Agreement.

High-Risk Partner

A partner classified as high risk because of its activities, ownership, jurisdiction, payment flows, customer vulnerability, financial-crime exposure, technology access, adverse information or reputational profile.

Network Limit

The contractual, technical, geographic, category and operational restrictions applied to preserve the controlled nature of the partner network.

Partner Administrator

An individual authorised by an Approved Partner to manage its MoneySafe account and users.

Partner Agreement

The written agreement between MoneySafe and an Approved Partner.

Policy Owner

The person accountable for maintaining this Policy and coordinating its implementation.

Suspension

A temporary restriction on some or all partner activity while an issue is investigated or remediated.

Removal

Termination of the partner's participation and deactivation of its access.

---

5. Governance and accountability

5.1 Policy Owner

The Policy Owner is accountable for maintaining this Policy, ensuring admission records are complete, monitoring compliance, coordinating material escalations and ensuring periodic reviews occur.

5.2 Partner Operations

Partner Operations coordinates applications, collects and validates admission documents, completes the admission checklist, maintains the Partner Register, coordinates onboarding and testing, and ensures that no Applicant is activated before approvals are complete.

5.3 Legal and Compliance

Legal/Compliance interprets this Policy, reviews restricted jurisdictions and categories, conducts or oversees enhanced due diligence, assesses limited-network and regulatory implications, approves or rejects permitted exceptions, reviews material changes and recommends suspension, removal or regulatory escalation.

5.4 Technology and Information Security

Technology/Security reviews integration architecture, approves access models, configures whitelists, validates security controls, approves production activation and disables access when a partner is restricted, suspended or removed.

5.5 Finance

Finance validates settlement details, verifies bank-account ownership, confirms invoicing and tax information, approves settlement readiness and reconciles partner redemptions and reimbursements.

5.6 Senior Approver

The Senior Approver is the person designated by MoneySafe management to approve medium- and high-risk partners, material exceptions and other decisions reserved under the approval matrix.

5.7 Conflicts of interest

Anyone involved in an admission or enforcement decision must disclose a personal, financial or business conflict of interest and must not approve the relevant matter unless an independent decision-maker authorises participation.

---

6. Admission lifecycle and approval gates

An Applicant must pass each applicable gate before proceeding to the next stage.

> **Gate 1 — Initial eligibility**
> Partner Operations confirms that the Applicant is legally established, has a lawful and eligible activity, operates in an approved or reviewable jurisdiction, can provide the required information and has no immediately disqualifying issue.

Gate 2 — Due diligence and risk classification

Reviewers verify identity, ownership, business activity, jurisdiction, settlement details, technical model and risk profile. A risk classification must be assigned before approval.

Gate 3 — Commercial and legal approval

Eligible Offers, customer-facing conditions, the Partner Agreement and any required data-processing terms must be approved.

Gate 4 — Settlement approval

Finance verifies the nominated business bank account, account ownership, invoicing details and reconciliation process.

Gate 5 — Technical approval

Technology/Security confirms the integration method, access roles, whitelist configuration, logging, testing and security requirements.

Gate 6 — Final activation

The authorised approver confirms that all required gates are complete. Only then may the partner be activated and accept redemptions.

No Applicant may advertise itself as an Approved Partner or accept MoneySafe redemptions before final activation.

---

7. Eligibility and due-diligence requirements

7.1 Minimum eligibility standard

- Be legally established and authorised to conduct its stated business.

- Provide its legal name, registration number and registered address.
- Identify directors, authorised representatives and beneficial owners where required.
- Operate within an approved product or service category.
- Lawfully provide its goods or services in the relevant jurisdiction.
- Demonstrate that it can honour proposed Eligible Offers.
- Maintain accurate redemption and settlement records.
- Meet MoneySafe's technical and security requirements.
- Agree to the Partner Agreement and applicable programme rules.
- Present no unacceptable legal, regulatory, financial-crime, consumer or reputational risk.

MoneySafe may request additional information whenever the Applicant's ownership, activities, jurisdiction, transaction profile or integration warrants enhanced review.

7.2 Admission file

Corporate information

- Legal name and trading name; registration or incorporation number; registered address and operating locations; tax or VAT number; website and public profiles; business contacts; directors and authorised signatories; beneficial ownership; ownership structure; and authority to enter into the Partner Agreement.

Business information

- Description of goods and services; proposed Eligible Offers; customer groups and delivery channels; operating countries and locations; expected redemption volumes; refund and cancellation practices; subcontractors or fulfilment partners; licences and permits; and insurance coverage where appropriate.

Settlement information

- Nominated business bank account; account-holder name; bank and country; evidence of account ownership; settlement contact; invoicing details; and applicable tax documentation.

Technical information

- Proposed integration method; point-of-sale, web or application environment; technical contacts; domains, IP addresses or callback endpoints; requested user roles; security controls; data-processing arrangements; and testing and certification requirements.

7.3 Prohibited or presumptively ineligible activities

MoneySafe will not ordinarily admit businesses whose principal activity involves unlawful goods or services, counterfeit or infringing goods, unlicensed financial services, unauthorised money transmission or electronic-money issuance, anonymous financial products designed to conceal ownership, adult sexual services, illegal gambling, weapons or controlled substances, trafficking or exploitation, deceptive investment or recruitment schemes, high-pressure or misleading sales practices, sanctions evasion, material unresolved enforcement action, or activity incompatible with customer safety, applicable law or the MoneySafe brand.

MoneySafe may reject a lawful Applicant where participation would create disproportionate risk or undermine the limited-network structure.

---

8. Risk classification

Each Applicant must be assigned a risk classification before final approval. The classification determines due diligence, approval authority, monitoring and review frequency.

8.1 Standard risk

May apply where the business is established in an approved jurisdiction, ownership and management are transparent, offerings are ordinary consumer products or services, expected redemption volumes are modest, settlement is

ordinary, technical access is limited and no material adverse information is identified.

8.2 Medium risk

May apply where there is a complex ownership or operating structure, large customer base or expected volume, cross-border activity, increased refund, fraud or complaint exposure, sensitive customer data, an untested business model, a higher-risk category or material dependence on subcontractors or intermediaries.

8.3 High risk

May apply where there is a high-risk category or jurisdiction, opaque ownership, adverse regulatory, litigation or media information, significant financial-crime exposure, vulnerable customers, high-value or unusually rapid redemptions, elevated chargeback or fraud risk, extensive technical or data access, or material risk to the Network Limit.

High-risk Applicants require enhanced due diligence and Senior Approver approval. MoneySafe may decline a High-Risk Partner where risk cannot be reduced to an acceptable level.

8.4 Risk factors

- Legal existence and authority
- Ownership and control
- Business activity
- Location and jurisdiction
- Regulatory status
- Sanctions and financial-crime exposure
- Customer vulnerability
- Complaints and enforcement history
- Fraud and chargeback risk
- Data protection and cybersecurity
- Operational resilience
- Financial capacity to honour offers
- Expected redemption volume

- Settlement and bank-account risk
- Subcontracting
- Reputational impact
- Effect on the Network Limit

---

9. Approval authority and decision matrix

Decision	Standard risk	Medium risk	High risk or exception
Initial eligibility review	Partner Operations	Partner Operations and Compliance	Compliance-led enhanced review
Due diligence sign-off	Partner Operations Manager	Compliance	Compliance and Senior Approver
Contract approval	Approved template owner	Legal/Compliance review	Legal/Compliance approval
Settlement approval	Finance	Finance and Compliance	Finance and Senior Approver
Technical activation	Technology	Technology and Security	Security and Senior Approver
Final partner admission	Partner Operations Manager	Senior Approver	Senior Approver and Legal/Compliance
Material change	Relevant owner	Compliance review	Senior Approver and Legal/Compliance
Suspension	Policy Owner or incident lead	Policy Owner and Compliance	Immediate authorised action with prompt escalation

Removal	Policy Owner and Legal/Compliance	Senior Approver and Legal/Compliance	Senior Approver and Legal/Compliance

No approval may be granted by a person who has an unresolved conflict of interest.

---

10. Permitted jurisdictions

10.1 Approved jurisdictions

MoneySafe may admit partners established and operating in Greece, European Union Member States, European Economic Area countries, and other jurisdictions expressly approved in writing by Legal/Compliance and the Senior Approver. Approval of a jurisdiction does not automatically approve every business or activity located there.

10.2 Restricted jurisdictions and cross-border risk

Enhanced review is required where a partner is incorporated, controlled or managed in a jurisdiction subject to heightened financial-crime or sanctions risk, serves customers from a restricted jurisdiction, uses a bank account in another country, has complex cross-border settlement, relies on restricted intermediaries, or is subject to export, sanctions or trade restrictions.

MoneySafe may restrict customers, offers, settlement routes or technical access even where the partner itself is admitted.

10.3 Prohibited jurisdictions and locations

MoneySafe will not knowingly admit or maintain a partner where sanctions prohibit the relationship, the partner or beneficial owner is a prohibited person, the relationship would breach applicable law or provider requirements, the business cannot lawfully provide services in the location, or risks cannot be adequately controlled.

The approved-jurisdiction list must be maintained by Compliance and reviewed whenever law, sanctions, payment-provider rules or supervisory expectations change.

10.4 Expansion into a new jurisdiction

A partner must disclose all jurisdictions in which it will provide goods or services, advertise Eligible Offers, accept redemptions, collect customer data or receive settlement. No partner may expand into a new country through the MoneySafe Programme without prior written approval and, where necessary, updated contractual, tax, data-protection and regulatory analysis.

---

11. Permitted product and service categories

11.1 General rule

A partner’s products and services must be lawful, clearly described, suitable for customer-facing promotional offers and compatible with the closed-loop nature of the programme. MoneySafe may approve an entire category, a defined subset or a specific offer. The approved scope must be recorded in the Partner Register.

11.2 Generally permitted categories

Subject to due diligence and applicable law, generally permitted categories may include hospitality and dining; cafés, restaurants and food services; travel-related services; leisure and entertainment; retail goods; personal care and wellness; professional services; education and training; home and lifestyle services; transport and mobility; cultural and community activities; and other ordinary consumer goods or services approved by MoneySafe.

This list is illustrative and does not create an automatic right of admission.

11.3 Restricted categories

Enhanced review and written approval are required for health, medical, dental or therapeutic services; financial education or credit-related services; insurance-related services; prepaid travel packages; subscriptions; high-value goods; marketplaces; services involving children or vulnerable customers; sensitive personal-data services; digital or virtual goods; elevated cancellation or delivery-risk services; regulated professional services; and categories designated restricted by MoneySafe, a payment provider or a competent authority.

11.4 Prohibited categories

MoneySafe will not approve offers involving money, electronic money or payment services; cash withdrawal or cash-equivalent instruments; customer-to-customer transfers; unlicensed lending, investment or wealth products; cryptocurrencies or virtual-asset services unless separately approved; unlawful gambling or betting; weapons, controlled substances or illegal goods; counterfeit products; adult sexual services; deceptive health claims; pyramid, Ponzi or recruitment schemes; unlawful goods or services; misleading or unsafe promotions; or any offer that could make MoneySafe Wallet appear to be a general-purpose payment product.

11.5 Eligible Offer approval

Each Eligible Offer must state clearly the included product or service, discount or benefit, price or pricing basis, eligibility conditions, location and time restrictions, expiry date, exclusions, cancellation and refund treatment, redemption steps and customer-support route.

MoneySafe may reject an offer that is technically eligible but unsuitable for customer presentation or inconsistent with the Network Limit.

---

12. Technical onboarding and whitelisting

12.1 Activation prerequisites

A partner may not accept MoneySafe redemptions based solely on an email, verbal approval, marketing commitment or payment of a fee.

1. Completed admission review
2. Assigned risk classification
3. Required approvals
4. Executed Partner Agreement
5. Verified settlement details
6. Approved technical integration
7. Successful testing
8. Activation by an authorised MoneySafe administrator

12.2 Approved integration methods

MoneySafe may support a partner dashboard, QR or token redemption, secure API, approved point-of-sale integration, controlled web interface or another method approved by Technology and Security.

The integration must reliably record partner identity, offer identity, redemption timestamp, customer or transaction reference where lawful and necessary, value or benefit applied, reversal or cancellation status and responsible user or system.

12.3 Identity and access management

MoneySafe will create a unique partner identifier, verify the Partner Administrator, apply role-based access, require strong authentication where appropriate, maintain access logs, prohibit shared credentials, review administrator access periodically and deactivate access promptly when personnel change or the partner is restricted.

Partners must notify MoneySafe without undue delay of changes to administrators, credentials, endpoints or security incidents.

12.4 Whitelisting controls

Whitelisting may cover the approved legal entity and partner identifier, trading locations, domains, callback URLs, IP addresses, application identifiers, offer identifiers, products or categories and settlement account. No redemption may be accepted outside the approved whitelist unless an authorised exception is documented and technically controlled.

12.5 Testing and certification

Before production activation, the partner must complete testing for authentication, valid redemption, duplicate prevention, invalid or expired offers, reversals and refunds, settlement and reconciliation, access roles, error handling, logging, data minimisation and suspension or deactivation behaviour.

12.6 Change management

Prior written approval is required before changing the legal entity or ownership, settlement account, domain, application or endpoint, technical architecture, offer, category, jurisdiction, redemption flow, subcontractor, data-processing

arrangement or any feature affecting the Network Limit. Emergency changes may be applied to protect customers or systems but must be documented and reviewed promptly.

12.7 Data and security requirements

The partner must process only necessary data, protect credentials and customer information, maintain reasonable security controls, notify MoneySafe promptly of suspected incidents, cooperate with containment and investigation, not sell or repurpose MoneySafe customer data, and comply with applicable privacy terms.

---

13. Contractual minimum requirements

Every Approved Partner must sign the current MoneySafe Partner Agreement before activation.

The agreement must include, at minimum:

13.1 Parties, scope and authority

Legal names and registration details, registered addresses, authorised signatories, approved services, approved locations and jurisdictions, and term and renewal provisions.

13.2 Programme restrictions

Acceptance only of approved Eligible Offers; no representation of MoneySafe Wallet as a bank account, electronic money or general-purpose payment product; no creation, sale, transfer or cash-out of points; no unauthorised sub-partners; no redemption outside the approved technical process; and compliance with the Network Limit.

13.3 Offer and customer obligations

Accurate offer description, honouring valid redemptions, clear exclusions and expiry terms, fair and non-misleading communications, customer-support and complaint cooperation, refund and cancellation responsibilities, and treatment of unavailable offers.

13.4 Redemption and settlement

Evidence for valid redemption, duplicate and fraud prevention, reconciliation procedures, settlement timing, fees and deductions, invoice or settlement statement requirements, reversals and chargebacks, disputes and correction of settlement errors.

13.5 Compliance and financial crime

Compliance with applicable law, sanctions and prohibited-person controls, anti-bribery and anti-corruption requirements, prohibition of unlawful or deceptive activity, cooperation with compliance checks, and notification of investigations or enforcement action.

13.6 Data protection and security

Permitted data processing, confidentiality, security safeguards, breach notification, retention and deletion, subprocessor controls, audit cooperation and allocation of data-protection responsibilities.

13.7 Audit and information rights

Rights to request records, access relevant systems and locations, obtain enhanced access where breach, fraud or regulatory requirements arise, enforce retention, assist with complaints and investigations, and cooperate with providers and authorities.

13.8 Liability, insurance and subcontractors

Responsibility for products, services and advertising; responsibility for inaccurate or unauthorised redemptions; risk-appropriate indemnities; liability limitations subject to mandatory law; insurance requirements; and responsibility for subcontractors.

13.9 Suspension and termination

Immediate suspension rights, termination for breach or legal and reputational risk, inactivity or network rationalisation, post-termination redemption rules, return or deletion of materials and data, final settlement and reconciliation, and continuing confidentiality and audit obligations.

14. Monitoring and audit

14.1 Monitoring framework

MoneySafe will operate a risk-based monitoring programme covering partner status and ownership, permitted activities and jurisdictions, complaints, redemption patterns, duplicates or unusual redemptions, chargebacks and refunds, failed settlement, offer accuracy, technical access, security incidents, adverse information and changes affecting the Network Limit.

14.2 Redemption monitoring

MoneySafe may monitor for unusual volume or velocity, repeated redemptions, out-of-hours activity, excessive reversals, abnormal discount rates, inconsistent redemptions, repeated use of devices or tokens, unapproved locations, settlement mismatches and suspected collusion or manipulation.

14.3 Periodic partner review

Risk classification	Minimum review frequency
Standard risk	At least every 24 months
Medium risk	At least annually
High risk	At least annually, with enhanced interim monitoring

A review may occur sooner after a complaint or incident, ownership change, jurisdiction or category change, abnormal activity, payment-provider concern, adverse information, security incident or material programme change.

14.4 Audit rights

Subject to law and the Partner Agreement, MoneySafe may request corporate, operational, settlement and redemption records; verify legal status and bank-account ownership; review offers and communications; test redemption; inspect controls and logs; conduct remote or on-site audits; require corrective-action plans; appoint an independent auditor; and share relevant information with advisers, providers or authorities where permitted or required.

Where there is a suspected serious breach, fraud, security incident or legal requirement, MoneySafe may conduct an urgent audit without the ordinary notice period.

14.5 Record retention

Partners must retain records evidencing valid redemptions, refunds and reversals, settlement calculations, complaints, staff or system access, relevant security events and compliance with the Partner Agreement. The applicable retention period will be stated in the Partner Agreement and must meet mandatory legal requirements.

14.6 Corrective action

MoneySafe may require clarification or documents, staff retraining, offer changes, technical remediation, enhanced reconciliation, restricted locations or hours, reduced limits, increased reporting, a corrective-action plan or suspension until remediation is complete.

---

15. Suspension, reinstatement and removal

15.1 Grounds for suspension

MoneySafe may suspend activity for breach, inaccurate information, expired licences, payment or settlement issues, fraudulent or manipulated redemptions, failure to provide advertised benefits, security or data incidents, unapproved jurisdictions or categories, unauthorised ownership change, sanctions or reputational risk, risk to the Network Limit, failure to cooperate, insolvency or a provider or authority requirement.

15.2 Immediate protective suspension

MoneySafe may immediately suspend a partner account, user, offer, location, settlement account, technical endpoint or redemption/issuance activity where necessary to protect customers, funds, systems, evidence or regulatory compliance. The incident lead must document the reason, scope, time and approving authority and escalate to the Policy Owner and Compliance.

15.3 Standard suspension workflow

1. **Identify** the issue, source and evidence.
2. **Assess** severity, customer impact, legal impact and network impact.
3. **Decide** whether to monitor, restrict, suspend or remove.
4. **Notify** the partner unless notification creates legal, investigative or security risk.
5. **Contain** affected offers, users, locations or endpoints.
6. **Investigate** records, logs, complaints, settlements and explanations.
7. **Remediate** through a corrective-action plan where appropriate.
8. **Reassess** reinstatement, restriction or removal.
9. **Document** the final decision, evidence and follow-up owner.

15.4 Partner response

The partner may be required to provide an explanation, records, remediation evidence, revised communications, an incident report, updated ownership or licence records, reconciliation statements or a recurrence-prevention plan. Failure to respond may result in removal.

15.5 Reinstatement

Reinstatement requires confirmation that the cause was addressed, customer impact remedied, technical controls tested, settlements reconciled, documents updated, Legal/Compliance has no unresolved objection and the authorised approver has approved reactivation. Enhanced monitoring, reduced limits or probation may apply.

15.6 Grounds for removal

MoneySafe may remove a partner for serious or repeated breach, fraud, deception or unlawful conduct, falsified information, failed remediation, loss of legal authority, prohibited category or jurisdiction, unacceptable ownership risk, compromised security, inability to honour or settle, risk to the Network Limit, provider or authority requirement, or customer or programme protection.

15.7 Removal workflow

1. Approval under the authority matrix.

2. Notice to the partner unless prohibited or impracticable.
3. Deactivation of accounts, users, offers and endpoints.
4. Removal from customer-facing directories.
5. Preservation of relevant records.
6. Reconciliation of redemptions, refunds, chargebacks and settlement.
7. Customer communication where necessary.
8. Return, deletion or restriction of data and MoneySafe materials.
9. Update of the Partner Register.
10. Post-removal review for related partners, offers or risks.

15.8 Open customer redemptions

When a partner is suspended or removed, MoneySafe will consider the Customer Terms, offer conditions, reason for action, ability to honour valid offers, consumer law, substitute arrangements and customer-harm risk. Material changes must be communicated clearly.

15.9 Reconsideration

Where appropriate, a suspended or removed partner may request reconsideration by providing new evidence or demonstrating remediation. A request does not automatically restore access, and the decision-maker should be independent where reasonably practicable.

---

16. Partner Register and records

MoneySafe must maintain a controlled Partner Register containing:

- legal identity and approved trading names;
- risk classification;
- approved jurisdictions, categories, locations and offers;
- contract status and dates;
- settlement account;
- technical integration and whitelist details;
- approval authorities;

- monitoring status;
- suspension or removal history; and
- next review date.

The Register must be access-controlled and current. No partner may remain active where it shows an expired agreement, missing approval, incomplete technical activation or overdue mandatory review.

---

17. Exceptions

Exceptions require written approval before activation or continued participation.

An exception request must state the requirement, reason, duration, risks, compensating controls, effect on the Network Limit, approving authority and review or expiry date.

No exception may authorise unlawful activity, sanctions violations, misleading customer communications, cash-out, customer-to-customer transfer or unrestricted payment functionality.

---

18. Reporting and escalation

The following matters must be escalated promptly to the Policy Owner and Compliance:

- suspected fraud or collusion;
- material customer harm;
- sanctions or prohibited-person concerns;
- serious security or privacy incidents;
- unexplained settlement discrepancies;
- repeated complaints;
- unauthorised category or jurisdiction expansion;
- material ownership change;
- regulatory or law-enforcement contact;

- evidence that the network is becoming effectively unrestricted; or
- any feature that could make MoneySafe Wallet operate as a general-purpose payment product.

Where required, MoneySafe will notify payment providers, insurers, regulators, customers or other affected parties.

---

19. Admission and activation checklist

Before activating a partner, the responsible team must confirm:

☐ Legal name and registration verified.

☐ Registered address and operating locations verified.

☐ Ownership and beneficial ownership reviewed where required.

☐ Directors and authorised representatives verified.

☐ Business activity and proposed offers reviewed.

☐ Jurisdiction approved.

☐ Product or service category approved.

☐ Risk classification assigned.

☐ Sanctions and adverse-information checks completed.

☐ Settlement bank account verified.

☐ Partner Agreement signed.

☐ Data-protection terms completed.

☐ Technical integration approved.

☐ Whitelist configured.

☐ User roles and authentication configured.

☐ Test transactions completed successfully.

☐ Refund, reversal and dispute process confirmed.

☐ Customer-facing offer approved.

☐ Monitoring thresholds configured.

☐ Review date recorded.

☐ Final activation authorised.