

AML & Compliance Policy

Last updated: 7 August 2026

1. Introduction

Fundscrow is committed to maintaining a comprehensive and risk-based compliance framework designed to prevent money laundering, terrorist financing, sanctions evasion, fraud, financial crime and the misuse of digital assets.

Protecting the integrity of the Fundscrow platform is fundamental to our business. Our compliance programme is designed to safeguard our customers, authorised service providers, payment partners, blockchain infrastructure and the wider financial system whilst allowing legitimate customers to access digital asset services through a secure and efficient platform.

This AML & Compliance Policy explains the principles, controls and procedures applied by Fundscrow in connection with the services offered through the platform. It applies to all customers, whether acting as private individuals or businesses, and covers every service provided by Fundscrow, including digital asset wallets, escrow services, cryptocurrency swaps, on-ramp services, off-ramp services, virtual payment cards, business accounts, mass payouts, API services and any additional products introduced in the future.

Fundscrow applies a continuous risk-based compliance model rather than relying solely on identity verification during account registration. Customer activity is assessed throughout the entire relationship using automated monitoring systems, blockchain analytics, behavioural analysis, transaction monitoring, sanctions screening, fraud detection technologies and internal compliance procedures designed to identify elevated risk.

Unlike many traditional financial institutions, Fundscrow does not normally require every customer to complete document-based identity verification before accessing standard platform services. Our approach is based upon proportionality and risk. Customers presenting a low level of risk may continue using the platform without additional verification, whilst customers or transactions presenting elevated risk may be subject to enhanced compliance reviews at any stage.

Fundscrow reserves the right to request additional information, supporting documentation or enhanced verification whenever reasonably necessary to comply with applicable laws, fulfil contractual obligations, satisfy authorised infrastructure providers, investigate suspicious activity or protect the integrity of the platform.

Compliance reviews may take place before an account is activated, during normal account use, before or after individual transactions, during escrow arrangements, before virtual card funding, during on-ramp or off-ramp transactions, when using API services or at any other time that Fundscrow considers reasonably necessary.

Our compliance framework is continually reviewed and enhanced to reflect changes in financial crime risks, blockchain technology, regulatory expectations, sanctions programmes, industry best practice and the operational requirements of our authorised service providers.

Nothing in this AML & Compliance Policy limits Fundscrow's right to delay or refuse transactions, request additional verification, suspend individual services, restrict account functionality, terminate customer relationships or take any other reasonable action necessary to comply with applicable law or protect the security, reputation and lawful operation of the Fundscrow platform.

This AML & Compliance Policy forms part of the legal agreement between you and Fundscrow and should be read together with the Terms and Conditions, Privacy Policy, Risk Disclosure, Refund & Disputes Policy and Cookies Policy.

2. Our compliance approach

Fundscrow applies a comprehensive risk-based compliance framework designed to identify, assess and manage financial crime risks throughout the entire customer relationship. Our objective is to maintain a secure digital asset ecosystem whilst providing a straightforward experience for legitimate customers.

Rather than relying solely on verification during account registration, Fundscrow continuously monitors customer activity, transaction behaviour and operational risk across all services available through the platform. This approach allows compliance measures to be applied proportionately according to the level of risk presented by each customer, account and transaction.

Our compliance framework combines automated technology with internal compliance procedures. These controls may include transaction monitoring, blockchain analytics, sanctions screening, fraud detection, behavioural analysis, device intelligence, risk scoring, account monitoring and other security measures designed to protect the platform and its users.

The level of monitoring applied to an account may change over time based on transaction patterns, wallet activity, escrow transactions, virtual card usage, cryptocurrency swaps, on-ramp and off-ramp activity, API usage, geographical indicators, security events or any other factors considered relevant to the overall risk profile.

Customers presenting a lower level of risk may continue using Fundscrow without additional verification. Where elevated risk is identified, Fundscrow may require enhanced due diligence before allowing certain services or transactions to continue.

Enhanced compliance measures may include requests for proof of identity, proof of address, source of funds, source of wealth, business documentation, ownership of digital assets, transaction information or any other documentation reasonably required to complete a compliance assessment.

Fundscrow does not rely upon fixed rules or one-time customer checks. Risk assessments are dynamic and continue throughout the entire customer relationship. Compliance decisions are based on the totality of the information available at the relevant time rather than any single event or transaction.

Where necessary to protect the platform, Fundscrow reserves the right to delay or refuse transactions, restrict specific services, suspend account functionality or terminate customer relationships where continued access would expose Fundscrow, its customers or its authorised service providers to unacceptable legal, regulatory, financial, operational or reputational risk.

Compliance decisions are supported by both automated systems and, where appropriate, manual review by authorised personnel. For security reasons, Fundscrow does not disclose the internal operation of its compliance systems, monitoring thresholds, risk models or decision-making methodologies, as doing so could compromise the effectiveness of the controls implemented to protect the platform.

Fundscrow continually reviews and strengthens its compliance programme to reflect changes in financial crime trends, blockchain technology, international sanctions programmes, regulatory expectations, industry standards and the evolving nature of digital asset services. This ongoing approach enables Fundscrow to maintain a compliance framework that remains effective, proportionate and appropriate as the platform and the wider digital asset industry continue to develop.

4. Transaction monitoring

Transaction monitoring is a fundamental part of Fundscrow's compliance programme and applies to all products and services available through the platform.

Fundscrow continuously monitors customer activity to identify unusual behaviour, reduce financial crime risk and protect the integrity of the Fundscrow ecosystem. Monitoring is performed throughout the entire customer relationship and is not limited to account registration or individual transactions.

Automated monitoring systems and internal compliance procedures assess activity across digital asset wallets, escrow transactions, cryptocurrency swaps, virtual card funding and spending, on-ramp services, off-ramp services, business accounts, mass payouts, API activity and other services provided through the platform.

Monitoring may include the assessment of transaction values, transaction frequency, wallet behaviour, blockchain activity, counterparty risk, geographical indicators, merchant activity, account access patterns, device information, API requests and historical customer behaviour.

Transactions are evaluated individually and collectively to identify activity that may be inconsistent with a customer's expected use of the platform or which presents an increased compliance, operational or security risk.

Where activity remains consistent with the customer's normal profile and presents a low level of risk, transactions will normally continue without interruption.

Where elevated risk is identified, Fundscrow may delay, decline or suspend transactions whilst additional reviews are completed. We may also request further information or supporting documentation before allowing the transaction to proceed.

Transaction monitoring may identify circumstances including unusually large transactions, rapid increases in activity, multiple linked transactions, unusual wallet movements, repeated failed transactions, abnormal virtual card usage, higher-risk jurisdictions, blockchain addresses presenting elevated risk, unusual escrow activity, suspicious API usage or other behaviour that differs materially from the customer's normal activity.

The identification of unusual activity does not automatically indicate unlawful conduct. Many alerts are generated through routine monitoring and are resolved following standard compliance reviews without further action.

For security reasons, Fundscrow does not disclose the transaction thresholds, monitoring rules, alert parameters, blockchain analytics methodologies or internal risk models used within its compliance programme.

Fundscrow continually reviews and enhances its transaction monitoring systems to reflect emerging financial crime threats, changes in blockchain technology, evolving regulatory expectations, new platform services and improvements in compliance technology, ensuring that monitoring remains proportionate, effective and appropriate for the scale of the Fundscrow ecosystem.

5. Sanctions screening

Fundscrow maintains a comprehensive sanctions compliance programme designed to prevent the platform from being used by sanctioned individuals, organisations, jurisdictions or other parties subject to applicable sanctions programmes.

Sanctions screening forms part of Fundscrow's ongoing compliance framework and applies throughout the customer relationship. Screening is not limited to account registration and may be performed before, during or after the use of any Fundscrow service.

Fundscrow may screen customers, beneficial owners, authorised representatives, wallet addresses, blockchain transactions, counterparties, payment information, businesses and other relevant data against applicable sanctions lists, watchlists and internal risk databases.

Sanctions screening may also take place before processing wallet transactions, escrow releases, cryptocurrency swaps, virtual card funding, on-ramp transactions, off-ramp transactions, business account activity, API transactions and any other service provided through the Fundscrow platform.

Where potential sanctions exposure is identified, Fundscrow may temporarily delay or refuse transactions, suspend access to individual services, restrict account functionality or request additional information whilst the matter is reviewed.

The identification of a potential sanctions match does not automatically mean that a customer is subject to sanctions. Alerts may require further investigation before a final compliance decision can be reached.

Fundscrow reserves the right to refuse account registration, decline transactions, terminate customer relationships or discontinue the provision of services where continuing the relationship would expose Fundscrow, its customers or its authorised service providers to sanctions-related, legal or regulatory risk.

Fundscrow may also implement additional restrictions in response to changes in international sanctions programmes, regulatory guidance, government measures or contractual obligations imposed by authorised infrastructure providers.

For security and compliance reasons, Fundscrow does not disclose the detailed operation of its sanctions screening systems, screening providers, matching algorithms, risk thresholds or internal decision-making processes.

Where required by applicable law, Fundscrow may cooperate with competent authorities, regulators, law enforcement agencies, payment networks, blockchain analytics providers and authorised service providers in relation to sanctions compliance or investigations into suspected unlawful activity.

Fundscrow continually reviews its sanctions compliance programme to ensure that it remains effective, proportionate and aligned with evolving international sanctions regimes, regulatory expectations and the operational requirements of the Fundscrow platform.

6. Source of funds and source of wealth

Fundscrow may request information regarding the source of funds or, where appropriate, the source of wealth where this is reasonably necessary to satisfy our compliance obligations, manage financial crime risks or protect the integrity of the platform.

Such requests are not routinely made for every customer. Fundscrow applies a risk-based approach, meaning that additional information is only requested where customer activity, transaction patterns, business relationships or other relevant circumstances indicate that further review is appropriate.

Source of funds refers to the origin of the specific digital assets or fiat funds used in a particular transaction or series of transactions. Source of wealth refers to the origin of a customer's overall financial position or accumulated assets where this information is reasonably required as part of an enhanced compliance assessment.

Fundscrow may request supporting information in connection with digital asset wallets, escrow transactions, cryptocurrency swaps, virtual card funding, on-ramp services, off-ramp services, business accounts, mass payouts, API services or any other product available through the platform.

Supporting information may include blockchain transaction references, exchange statements, invoices, contracts, proof of business activities, bank statements, proof of asset

ownership, tax documentation or any other information reasonably required to understand the origin of the relevant assets or funds.

The information requested will depend upon the nature of the customer relationship, the services being used, the value of the transactions involved and the overall level of risk identified during the compliance review.

Fundscrow reserves the right to delay, restrict or decline transactions until requested information has been received and appropriately reviewed. Where a customer fails to provide requested information within a reasonable period, Fundscrow may restrict services, suspend account functionality or terminate the customer relationship where appropriate.

The provision of source of funds or source of wealth information does not automatically result in the approval of a transaction or the continuation of services. All information is assessed as part of Fundscrow's overall compliance programme and risk management framework.

For security reasons, Fundscrow does not disclose the thresholds, methodologies or internal criteria used when determining whether source of funds or source of wealth information is required. These measures are reviewed regularly to reflect evolving financial crime risks, regulatory expectations and industry best practice.

All information provided as part of a compliance review is treated as confidential and processed in accordance with the Fundscrow Privacy Policy. Access is restricted to authorised personnel and retained only for as long as necessary to satisfy legal, regulatory, contractual, operational and security requirements.

7. Suspicious activity and reporting

Fundscrow is committed to preventing the misuse of its platform for money laundering, terrorist financing, fraud, sanctions evasion and other forms of financial crime. As part of this commitment, Fundscrow continuously monitors customer activity and investigates transactions or behaviour that present an elevated level of risk.

Suspicious activity may be identified through transaction monitoring, blockchain analytics, behavioural analysis, sanctions screening, fraud detection systems, security alerts, customer communications or information received from authorised service providers or competent authorities.

Activity that may require additional review includes, but is not limited to, unusually large or complex transactions, rapid movement of digital assets, inconsistent account behaviour, unusual escrow activity, repeated virtual card funding or spending patterns, suspicious on-ramp or off-ramp activity, high-risk blockchain exposure, attempts to circumvent platform controls or any activity that appears inconsistent with the customer's expected use of the Fundscrow platform.

The identification of unusual or suspicious activity does not automatically indicate unlawful conduct. Many alerts are generated as part of Fundscrow's routine monitoring processes and are resolved through standard compliance procedures.

Where a compliance review is required, Fundscrow may temporarily delay transactions, suspend individual services, restrict account functionality or request additional information before allowing activity to continue.

Customers may be asked to provide supporting documentation, transaction records, contracts, invoices, blockchain evidence, proof of wallet ownership, source of funds information or any other documentation reasonably required to complete the review.

Where Fundscrow reasonably believes that an account or transaction may involve unlawful activity, we reserve the right to refuse transactions, suspend services, terminate the customer relationship and take any other action reasonably necessary to protect the platform and comply with applicable legal obligations.

Where required by applicable law, Fundscrow may submit reports or disclose relevant information to competent authorities, regulators, law enforcement agencies or other authorised organisations without prior notice to the customer where such notification is prohibited or would prejudice an investigation.

For security reasons, Fundscrow does not disclose its internal investigation procedures, reporting thresholds, risk indicators or the criteria used when determining whether suspicious activity reports or other regulatory notifications are required.

Fundscrow continually reviews and enhances its financial crime controls to ensure that suspicious activity is identified and managed effectively whilst maintaining a fair, proportionate and risk-based approach for legitimate customers using the platform.

8. Restricted jurisdictions and prohibited activities

Fundscrow provides its services only in jurisdictions where it is legally and operationally permitted to do so. The availability of the Fundscrow platform may vary depending on applicable laws, sanctions programmes, regulatory requirements and the operational capabilities of our authorised service providers.

Fundscrow reserves the right to restrict, suspend or refuse access to the platform or to specific services in any jurisdiction where providing those services would be unlawful, expose Fundscrow to unacceptable legal, regulatory, financial or operational risk, or conflict with the requirements of our authorised infrastructure providers.

Customers are solely responsible for ensuring that their use of the Fundscrow platform complies with the laws and regulations applicable in the jurisdictions from which they access or use our services.

Fundscrow does not permit the use of its platform for unlawful, fraudulent or abusive purposes. Customers must not use any Fundscrow service to facilitate money laundering,

terrorist financing, sanctions evasion, fraud, tax evasion, identity theft, market manipulation or any other activity prohibited by applicable law.

The platform must not be used to purchase, sell, transfer or facilitate transactions involving illegal goods or services, stolen property, counterfeit products, malicious software, prohibited weapons, child exploitation material or any activity that may expose Fundscrow or its customers to legal or regulatory risk.

Customers must not knowingly deposit, transfer or withdraw digital assets connected with unlawful activity or attempt to conceal the origin, ownership or destination of assets through the use of wallets, escrow services, cryptocurrency swaps, virtual cards, on-ramp services, off-ramp services, business accounts or any other Fundscrow product.

Fundscrow also prohibits attempts to circumvent transaction limits, compliance reviews, sanctions controls, account restrictions, monitoring systems or any security measures implemented to protect the platform.

Where Fundscrow reasonably believes that an account or transaction is connected with prohibited activity or a restricted jurisdiction, we reserve the right to delay or refuse transactions, restrict individual services, suspend account access, terminate the customer relationship or take any other action reasonably necessary to protect the platform and comply with applicable legal or contractual obligations.

For security and operational reasons, Fundscrow does not publish a complete list of restricted jurisdictions or prohibited activities. These may change from time to time in response to changes in applicable laws, international sanctions programmes, regulatory expectations, payment network requirements or the operational requirements of our authorised service providers.

Nothing in this section limits Fundscrow's right to take immediate action where necessary to protect the integrity of the platform, safeguard customer assets or comply with applicable legal obligations.

9. Record keeping

Fundscrow maintains comprehensive records relating to customer accounts, transactions, compliance reviews and platform activity as part of its commitment to effective compliance, operational integrity and financial crime prevention.

Records are maintained to support the secure operation of the platform, investigate customer enquiries, prevent fraud, comply with applicable legal and regulatory obligations, respond to lawful requests from competent authorities and protect the legitimate interests of Fundscrow and its customers.

The information retained may include account registration details, wallet activity, blockchain transaction records, escrow transactions, cryptocurrency swaps, virtual card activity, on-ramp and off-ramp transactions, business account information, API activity, customer

communications, compliance reviews, verification records, fraud investigations and other information reasonably necessary for the operation of the Fundscrow platform.

Fundscrow may also retain technical information, including authentication records, security logs, access history, device information, system events and operational monitoring data to support cybersecurity, fraud prevention, business continuity and platform resilience.

Where additional compliance reviews are conducted, Fundscrow may retain supporting documentation provided by customers together with the results of internal assessments, compliance decisions and correspondence relating to the review.

Records are retained only for as long as reasonably necessary to satisfy legal, regulatory, contractual, operational and security requirements. The applicable retention period may vary depending on the nature of the information, the services used and the legal obligations that apply to Fundscrow.

Access to records is strictly limited to authorised personnel who require such access to perform their duties. Fundscrow applies appropriate technical and organisational safeguards designed to protect records against unauthorised access, alteration, disclosure, loss or destruction.

Where records are no longer required, Fundscrow will securely delete, anonymise or permanently destroy the information in accordance with its internal retention procedures and applicable legal requirements. Certain information may remain within encrypted backup systems or disaster recovery environments for a limited period before being permanently removed.

Fundscrow reserves the right to retain records for longer periods where reasonably necessary to investigate fraud, resolve disputes, respond to legal proceedings, comply with requests from competent authorities, enforce contractual rights or protect the security and integrity of the Fundscrow platform.

Accurate record keeping forms an essential part of Fundscrow's compliance framework and supports our commitment to maintaining a secure, transparent and professionally operated digital asset ecosystem.

10. Cooperation with authorities

Fundscrow is committed to complying with all applicable laws and cooperating with competent authorities where required by law or where reasonably necessary to protect the integrity of the platform and the wider financial system.

Where legally required, Fundscrow may provide information, documentation or transaction records to regulators, courts, law enforcement agencies, tax authorities or other competent governmental bodies acting within their lawful authority.

Fundscrow may also cooperate with authorised payment providers, card programme managers, blockchain analytics providers, financial institutions and other authorised service providers where such cooperation is necessary to investigate suspected financial crime,

prevent fraud, comply with legal obligations or protect the security of the Fundscrow platform.

Where permitted by law, Fundscrow will assess the validity and scope of any request before disclosing customer information. Only information reasonably necessary to satisfy the applicable legal or regulatory requirement will be disclosed.

In certain circumstances, Fundscrow may be legally prohibited from notifying a customer that information has been requested or disclosed. Where such restrictions apply, Fundscrow will comply with its legal obligations and may be unable to discuss the existence or nature of any investigation or request.

Fundscrow reserves the right to delay transactions, suspend services, restrict account functionality or preserve relevant records where reasonably necessary to comply with legal obligations, court orders, regulatory requirements or lawful requests from competent authorities.

Nothing in this AML & Compliance Policy limits Fundscrow's right to take immediate action where reasonably necessary to prevent financial crime, protect customer assets, preserve evidence, maintain platform security or comply with applicable law.

Fundscrow remains committed to balancing customer privacy with its legal and regulatory responsibilities. Any disclosure of customer information will be carried out in accordance with applicable law and the Fundscrow Privacy Policy, ensuring that customer information is handled responsibly, securely and only where there is a lawful basis for doing so.

11. Customer responsibilities

Customers play an important role in maintaining the integrity and security of the Fundscrow platform. By using any Fundscrow service, you agree to comply with this AML & Compliance Policy, the Terms and Conditions and all applicable laws and regulations.

You are responsible for providing accurate, complete and up-to-date information when creating your account and throughout your relationship with Fundscrow. If any information previously provided becomes inaccurate or changes materially, you must update your account or notify Fundscrow without undue delay.

Customers must only use Fundscrow for lawful purposes and must not knowingly use the platform in connection with fraud, money laundering, terrorist financing, sanctions evasion or any other unlawful activity.

You agree to cooperate with any reasonable request made by Fundscrow as part of a compliance review. This may include providing additional information, supporting documentation or explanations relating to your account, transactions or business activities where reasonably required.

Customers are responsible for ensuring that digital assets deposited into or transferred through the platform have been obtained lawfully and that they have the legal right to use, transfer or otherwise deal with those assets.

You must not attempt to bypass Fundscrow's compliance controls, monitoring systems, transaction limits, account restrictions or security measures. Any attempt to interfere with or circumvent these controls may result in immediate restrictions, suspension of services or termination of your account.

Customers remain responsible for maintaining appropriate security over their accounts, authentication methods and devices. You must notify Fundscrow immediately if you become aware of any unauthorised access, suspicious activity or security incident affecting your account.

Failure to comply with this AML & Compliance Policy or any reasonable compliance request may result in delayed transactions, restricted access to services, enhanced due diligence, suspension of account functionality or termination of the customer relationship where appropriate.

By continuing to use the Fundscrow platform, you acknowledge that compliance is an ongoing process and agree to cooperate with Fundscrow in maintaining a secure, transparent and legally compliant digital asset ecosystem.

12. Changes to this AML & Compliance Policy

Fundscrow reserves the right to amend, update or replace this AML & Compliance Policy at any time to reflect changes in applicable laws, regulatory expectations, financial crime risks, industry standards, technological developments or the services offered through the Fundscrow platform.

As the platform continues to evolve, Fundscrow may introduce new products, technologies or infrastructure partners, including additional wallet services, escrow solutions, payment products, digital asset services, business solutions, APIs or other functionality. Where these developments affect our compliance framework, this AML & Compliance Policy will be updated accordingly.

Fundscrow continually reviews its compliance programme to ensure that it remains proportionate, effective and aligned with current legal, regulatory and operational requirements. Changes may also be introduced to strengthen fraud prevention, sanctions compliance, transaction monitoring, customer due diligence or other compliance controls.

The latest version of this AML & Compliance Policy will always be published on the Fundscrow website together with the date on which it became effective.

Where changes materially affect customer rights or obligations, Fundscrow will, where reasonably practicable, provide notice through the platform, by email or through other appropriate communication channels.

Your continued use of the Fundscrow platform after an updated AML & Compliance Policy becomes effective constitutes your acceptance of the revised policy to the extent permitted by applicable law.

Nothing in this section limits Fundscrow's right to implement immediate changes where necessary to comply with applicable law, regulatory requirements, court orders, sanctions programmes, contractual obligations or security incidents.

13. Contact us

If you have any questions regarding this AML & Compliance Policy or Fundscrow's compliance framework, you may contact our compliance or customer support team through the official contact details published on the Fundscrow website or through your registered Fundscrow account.

Fundscrow will make reasonable efforts to respond to compliance-related enquiries promptly. However, for security, legal and operational reasons, we may be unable to disclose information relating to internal compliance procedures, transaction monitoring systems, sanctions screening methodologies, fraud detection controls, risk scoring models or ongoing investigations.

Where your enquiry relates to your account or a compliance review, Fundscrow may request additional information to verify your identity before providing account-specific information.

Nothing in this AML & Compliance Policy limits Fundscrow's obligations under applicable law or prevents Fundscrow from taking any action reasonably necessary to protect the platform, its customers, authorised service providers or the wider financial system.