DRIVEX STUDIOS SL – INTERNAL MONITORING & INVESTIGATION PROCEDURES

Confidential Internal Compliance Framework

Last updated: May 2026

1. Purpose of this Document

This Internal Monitoring & Investigation Procedures document establishes the internal compliance, moderation, escalation, investigation, reporting and enforcement framework implemented by DRIVEX STUDIOS SL (“DriveX Studios”, “DriveX”, “we”, “our” or “us”) in connection with the operation of the DriveX Studios platform.

This document is intended to support:

- platform safety;
- anti-fraud controls;
- payment-compliance obligations;
- anti-exploitation obligations;
- moderation governance;
- legal compliance;
- operational risk management;
- cooperation with payment processors, acquiring banks and card networks;
- compliance with Visa VIRP and Mastercard BRAM standards.

This document is an internal operational compliance document and may contain confidential compliance procedures, escalation methodologies and operational safeguards.

---

2. Scope of Application

These procedures apply to:

- all content published or distributed through the Platform;
- all creators, performers and professional content suppliers;
- moderation teams;
- compliance personnel;
- legal personnel;
- fraud-prevention personnel;
- third-party service providers acting on behalf of DriveX Studios.

These procedures apply before publication, during publication and after publication of content.

---

3. Governance and Responsibility Structure

DriveX Studios maintains a compliance governance structure intended to support:

- risk detection;
- escalation management;
- moderation consistency;
- legal compliance;
- payment-compliance obligations;
- platform integrity.

Internal responsibilities may include:

3.1 Compliance Function

Responsible for:

- onboarding review;
- policy enforcement;
- escalation management;
- compliance audits;
- authority cooperation;
- payment partner cooperation.

3.2 Moderation Function

Responsible for:

- content review;
- pre-publication checks;
- prohibited-content detection;
- user-report review;
- emergency escalations.

3.3 Fraud & Risk Function

Responsible for:

- fraud monitoring;
- suspicious-payment review;
- chargeback-risk analysis;
- account-risk detection;
- anti-abuse systems.

3.4 Legal Function

Responsible for:

- legal escalation review;
- authority requests;
- intellectual-property complaints;
- litigation support;

- evidence preservation.

---

4. Monitoring Framework

DriveX Studios implements a hybrid monitoring framework combining:

- automated monitoring systems;
- human moderation review;
- compliance escalation;
- fraud-detection systems;
- risk-based investigations;
- payment-risk analysis.

Monitoring measures may include:

- metadata analysis;
- upload-pattern monitoring;
- payment-risk monitoring;
- suspicious behavioral analysis;
- duplicate-content detection;
- prohibited-keyword detection;
- user complaints;
- trusted-flagger reports;
- account-behavior analysis.

Monitoring systems may be updated according to:

- evolving legal requirements;
- fraud trends;
- payment-processor expectations;
- card-network standards;
- platform-risk assessments.

---

5. Pre-Publication Review Procedures

All professional content uploaded or submitted to the Platform may be subject to pre-publication review.

Pre-publication review procedures may include:

- identity verification review;
- age-verification confirmation;
- consent verification;
- prohibited-content screening;
- metadata review;
- payment-compliance screening;
- anti-trafficking review;
- image-rights review;
- fraud-risk assessment.

DriveX Studios reserves the right to:

- reject content;
- suspend publication;
- request additional documentation;
- escalate content for enhanced review.

No content is guaranteed publication.

---

6. Post-Publication Monitoring

Content may remain subject to ongoing monitoring after publication.

Post-publication monitoring may include:

- user reports;
- moderation review;
- payment-risk alerts;
- fraud investigations;
- authority requests;
- trusted-flagger notifications;
- automated detection systems;
- periodic audits.

DriveX Studios reserves the right to remove or restrict content at any time.

---

7. High-Risk Escalation Categories

The following categories may trigger immediate or enhanced escalation:

- suspected CSAM;
- suspected minors;
- trafficking indicators;
- coercion indicators;
- non-consensual content;
- impersonation;
- deepfake sexual content;
- payment fraud;
- account takeovers;
- identity fraud;
- chargeback abuse;
- suspicious creator onboarding;
- law-enforcement requests;
- payment processor escalations.

High-risk matters may be prioritized for immediate review.

---

8. Investigation Procedures

DriveX Studios may conduct internal investigations where reasonably necessary to:

- assess policy violations;
- investigate fraud;
- investigate illegal conduct;
- investigate exploitation concerns;
- assess payment risk;
- comply with legal obligations;
- support platform integrity.

Investigations may include:

- review of logs;
- review of verification records;
- review of communications;
- review of moderation history;
- review of payment activity;
- review of onboarding documentation;
- interviews or requests for clarification;
- cooperation with service providers.

DriveX Studios reserves the right to conduct investigations confidentially.

---

9. Emergency Response Procedures

Where reasonably necessary, DriveX Studios may implement emergency measures including:

- immediate content removal;
- temporary suspension;
- permanent account termination;
- payout freezes;
- preservation of evidence;
- account lockdown;
- notification to authorities;
- escalation to payment processors.

Emergency action may occur before completion of a full investigation.

---

10. Fraud Prevention and Payment Monitoring

DriveX Studios may implement:

- transaction-risk scoring;
- suspicious-payment monitoring;
- velocity controls;
- chargeback monitoring;

- anti-abuse systems;
- account-authentication controls;
- geolocation analysis;
- device-risk analysis.

Suspicious activity may result in:

- delayed activation;
- payment restrictions;
- account suspension;
- enhanced verification requests.

DriveX Studios may cooperate with:

- payment processors;
- acquiring banks;
- card networks;
- anti-fraud providers.

---

11. Evidence Preservation and Audit Trails

DriveX Studios may preserve:

- moderation logs;
- access logs;
- payment records;
- complaint records;
- investigation notes;
- onboarding records;
- verification records;
- communications;
- enforcement history.

Records may be retained where reasonably necessary for:

- legal compliance;
- anti-fraud obligations;
- payment-compliance obligations;
- dispute resolution;
- legal defense;
- authority cooperation.

---

12. Cooperation with Authorities and Payment Partners

DriveX Studios may cooperate with:

- law enforcement authorities;

- regulators;
- child-protection authorities;
- payment processors;
- acquiring banks;
- card networks;
- anti-fraud organizations.

DriveX Studios may disclose or preserve information where reasonably necessary to:

- comply with legal obligations;
- investigate unlawful conduct;
- protect minors;
- prevent fraud;
- comply with payment-compliance obligations.

---

13. Internal Confidentiality and Access Controls

Internal compliance information, investigations and moderation records may be treated as confidential.

Access may be restricted to:

- authorized compliance personnel;
- legal personnel;
- fraud-prevention personnel;
- senior management;
- authorized service providers acting under confidentiality obligations.

DriveX Studios may implement:

- role-based access controls;
- authentication measures;
- logging systems;
- secure storage;
- encryption measures.

---

14. Training and Compliance Updates

DriveX Studios may implement internal training and compliance updates relating to:

- prohibited content;
- anti-trafficking obligations;
- moderation standards;
- fraud prevention;
- payment compliance;
- escalation procedures;
- platform safety.

Internal procedures may be updated according to:

- legal developments;
- operational risks;
- card-network standards;
- payment-processor requirements;
- compliance assessments.

---

15. Limitation of Liability

DriveX Studios implements commercially reasonable monitoring and investigation procedures but cannot guarantee:

- immediate detection of all violations;
- uninterrupted monitoring systems;
- complete elimination of fraud attempts;
- error-free moderation or investigation outcomes.

Professional content suppliers remain independently responsible for compliance with applicable laws and contractual obligations.

---

16. Document Control and Updates

DriveX Studios reserves the right to modify or update these procedures at any time.

Updated versions may be distributed internally or made available to relevant compliance partners where appropriate.

---

17. Internal Compliance Contacts

Compliance: compliance@drivexstudios.com

Legal: legal@drivexstudios.com

Fraud & Risk: risk@drivexstudios.com

Support: support@drivexstudios.com