Anti-Money Laundering (AML) Policy

Group policy

xstreco

Contents

Approved by	The Board of Directors of Xstreco AG
Issued by	Executive management
Issued on	01.09.2026
Version	2.1

1 Introduction

1.1 Purpose and Scope

1.1.1 Purpose of the Policy

This policy sets out how money laundering and terrorist financing are prevented, detected and addressed across the Group, and the controls that apply to counterparties, payments and records.

1.1.2 Scope and Applicability

This policy applies to all employees, directors, officers, and contractors under Xstreco's direct supervision, working for any Xstreco office or industrial asset directly or indirectly controlled or operated by Xstreco worldwide. Where the Group holds an interest in a joint venture that it does not control or operate, it uses its influence to encourage conduct consistent with this policy.

2 Policy Statement

2.1 Group's Stance on Anti-Money Laundering

Assisting, supporting, participating in or permitting money laundering or the financing of terrorism, or the concealment of criminal proceeds, is prohibited. Dealing knowingly with the proceeds of crime is prohibited, as is the facilitation of tax evasion. These standards apply to everyone subject to this policy and, where their contract so provides, to counterparties.

2.2 Legal Implications

Article 305bis of the Swiss Criminal Code makes money laundering an offence, and Article 102 paragraph 2 makes an undertaking liable, for the offences that provision lists, where it failed to take all the reasonable organisational measures required to prevent the offence, irrespective of the criminal liability of any natural person. The Group is not a financial intermediary at the date of this issue, so the due diligence duties of the Anti-Money Laundering Act do not apply to it as such, although that Act reaches dealers accepting cash above the thresholds it sets, with a lower threshold for trades in precious metals and gemstones applying from 1 October 2026, and would reach a Group entity that traded bank precious metals for its own account on a professional basis. The Transparency of Legal Entities Act, which takes effect on the same date, requires Swiss legal entities to report their beneficial owners to a federal register; this policy requires the compliance function to determine, on legal advice, what that Act requires of the Swiss entities of the Group. In Peru, Decreto Legislativo N.° 1106, as amended, makes money laundering an offence, including where the proceeds derive from illegal mining, and Ley N.° 30424, as amended, attributes administrative liability to legal persons for it; whether a Peruvian Group company is a reporting entity of the Financial Intelligence Unit (UIF-Perú) is addressed in section 9.2. Non-compliance with this policy, and the conduct it prohibits, may result in legal penalties, reputational damage, and internal disciplinary action, including termination.

3 Key Principles and Guidelines

3.1 Specific Principles or Guidelines

This policy requires the following principles to be applied:

(a) Customer Due Diligence (CDD): Due diligence proportionate to the risk a counterparty presents must be carried out before a business relationship begins, extending to beneficial owners where that risk warrants it.

(b) Enhanced Due Diligence (EDD): Enhanced due diligence must be applied to high-risk counterparties, including a counterparty that is or acts through a shell company, to politically exposed persons and to transactions involving high-risk jurisdictions.

(c) Transaction Monitoring: Transactions must be monitored for unusual patterns and for inconsistency with a counterparty's known profile.

(d) Sanctions Screening: Counterparties must be screened, on a risk basis, against the applicable restricted party lists. The requirements that apply to sanctions, export controls and restrictive measures, and to the screening, escalation and record keeping they call for, are set out in the Sanctions and Compliance Policy.

(e) Record Keeping: Records of transactions and of due diligence must be accurate and must be retained for the period the law applicable to them requires and, subject to that period, in accordance with the retention arrangements required by the Information Governance and Security Policy.

(f) Suspicious Activity Reporting: Suspicious activity must be reported to the compliance function without delay. The compliance function assesses each report and, having taken legal advice where appropriate, decides whether the matter must or may be reported to a competent authority, being the Money Laundering Reporting Office Switzerland where the Anti-Money Laundering Act so requires, the Financial Intelligence Unit (UIF-Perú) where Peruvian law so requires, and otherwise the prosecuting authorities.

3.2 Examples and Applications

(a) Cash Payment Out of Profile: A counterparty offers payment in cash on a scale inconsistent with its business profile. This must be reported to the compliance function as suspicious activity.

(b) Third-Party Laundering Risk: A supplier requests payment to an unrelated offshore account. This is a red flag and must be reported to the compliance function.

(c) Sanctions Screening Hit: Screening of a potential counterparty during onboarding returns a possible match against a restricted party. The dealing must be halted and the match escalated to the compliance function, and the relationship must not be entered into where the match is confirmed.

4 Roles and Responsibilities

4.1 The Board

Oversight of this policy rests with the board. The board approves this policy and each revision of it.

4.2 Executive Management

Executive management issues this policy, provides the means required to apply it, and is accountable to the board for its application. Where this policy requires a matter to be escalated, it is escalated to executive management.

4.3 Responsibility for This Policy

Responsibility for the day-to-day application of this policy is assigned within the Group. This policy requires that the assignment be recorded in the Schedule of Policy Assignments, an internal document, be kept current, and be made known to those subject to this policy. Where this policy refers to the compliance function, it means the person or persons holding that assignment at the relevant time, whether or not a separate department exists.

4.4 Those Who Direct the Work of Others

Anyone who directs the work of others is responsible for applying this policy in the work they direct, for making those they direct aware of it, and for passing on a concern raised with them.

4.5 Everyone Subject to This Policy

Everyone subject to this policy must comply with it, must raise a concern where they believe it has been or may be breached, and must co-operate with any enquiry into such a concern.

4.6 Counterparties

Counterparties must meet the standards in this policy where their contract with the Group so provides, and may raise a concern through the channels in section 5.1.

4.7 Those Responsible for Counterparties and Payments

Those responsible for engaging a counterparty, or for making or receiving a payment, are responsible for establishing who the counterparty is and where the funds come from, to the depth this policy requires, before the Group is committed, and for referring anything unexplained to the compliance function.

5 Reporting and Monitoring

5.1 Reporting Mechanisms

5.1.1 Internal Reporting

A concern under this policy may be raised with a line manager, with any member of executive management, or with the compliance function. A concern may also be raised through the web reporting form at xstreco.com/report, by writing to compliance@xstreco.com or codeofconduct@xstreco.com, both of which reach the compliance function, or by telephone on +41 41 562 32 90, asking for the compliance function. Retaliation against a person who raises a concern in good faith is prohibited.

5.1.2 External Reporting

A person who is not employed by the Group may raise a concern through the web reporting form at xstreco.com/report, by writing to compliance@xstreco.com or codeofconduct@xstreco.com, by telephone on +41 41 562 32 90, or by post, marked 'Confidential - Compliance', to the address at the end of this document. A concern may be raised in English or in Spanish. A name and contact details are not required, and a concern raised without them is assessed in the same way. The Group's website provider records basic technical data with every submission, so a report made through the form is not technically anonymous, and a call is not anonymous; a report sent by post can be.

5.2 Monitoring Procedures

This policy requires that its application be kept under review, and that a record sufficient to show how it has been applied be kept. In particular, this policy requires:

(a) that compliance with this policy be reviewed on the cycle stated in section 8;

(b) that concerns raised under this policy, and the way in which each was resolved, be recorded;

(c) that the risk this policy addresses be reassessed whenever the Group's activities change materially;

(d) that matters which are unresolved, which recur, or which are systemic be escalated to executive management and, where the law requires it or it is otherwise appropriate, to the competent authorities;

(e) that those subject to this policy be able to demonstrate, from the records kept, that its requirements were met.

The means used to meet these requirements are proportionate to the size of the Group and to the scale and nature of its activities at the time, and are extended as those change.

6 Training and Awareness

6.1 Awareness on Appointment

This policy requires that everyone subject to it be made aware of it on appointment and be given the instruction needed to apply it in their role. The form and the depth of that instruction are proportionate to the role.

6.2 Continuing Awareness

This policy requires that awareness of it be refreshed on the cycle stated in section 8, and whenever the policy is revised or an event makes it necessary, and that those in roles carrying greater exposure to the risk this policy addresses receive instruction appropriate to that exposure.

7 Compliance and Consequences

7.1 Reporting Non-Compliance

Everyone subject to this policy must report suspected violations, as must counterparties where their contract with the Group so provides. The identity of the person making a report is treated as confidential and is not disclosed except where disclosure is required by law or is necessary for the enquiry, and then only to the extent necessary. Retaliation against a person who reports in good faith is prohibited.

7.2 Consequences of Non-Compliance

Violations may result in disciplinary action, including termination of employment or contract, and may trigger legal proceedings.

8 Review and Revision

8.1 Review Frequency

8.1.1 Review Cycle

This policy is reviewed at least once in every two calendar years.

8.1.2 Event-Triggered Review

A review is carried out, whether or not one is due under the cycle, whenever a change in the law, a material change in the Group's activities, or an event arising under this policy makes one necessary.

8.1.3 Conduct and Outcome of the Review

The review is carried out by the holder of the responsibility described in section 4.3. Its outcome is submitted to the board, and any revision resulting from it is approved by the board before issue.

8.2 Revision History

8.2.1 Version 2.1 - 01.09.2026

Approved by the board and issued by executive management following a scheduled review of the suite. The amendments are editorial and clarifying; the policy positions stated in version 2.0 are unchanged.

8.2.2 Version 2.0 - 01.01.2026

Approved by the board and issued by executive management, replacing the first issue.

8.2.3 Version 1.0 - 02.06.2025

First issue.

8.2.4 Superseded Versions

Superseded versions are retained. Each revision is communicated to those subject to this policy.

9 Appendices

9.1 Glossary of Terms

(a) Money Laundering: The process of disguising the origins of illegally obtained money to make it appear legitimate.

(b) Beneficial Owner: The natural person who ultimately owns or controls an account, entity or transaction.

(c) Suspicious Activity: Any transaction or behaviour that raises doubts about its legality or legitimacy.

(d) Due Diligence: The process of assessing the integrity and compliance of third parties.

(e) PEP (Politically Exposed Person): A person entrusted with a prominent public function, in Switzerland or abroad or in an international organisation, together with that person's family members and close associates. A relationship with a PEP requires enhanced due diligence.

(f) Sanctions Screening: The process of checking individuals or entities against the applicable restricted party lists.

(g) Shell Company: A legal entity with no significant assets or operations; its use by a counterparty requires enhanced due diligence under section 3.1.

9.2 Related Legislation

9.2.1 Local Legislation

In Switzerland, Article 305bis of the Criminal Code, Article 102 on corporate criminal liability, the Anti-Money Laundering Act (SR 955.0) and the Transparency of Legal Entities Act, which takes effect on 1 October 2026. In Peru, Decreto Legislativo N.° 1106, as amended, on the effective fight against money laundering and offences related to illegal mining and organised crime, and Ley N.° 30424, as amended, on the administrative liability of legal persons. Obligations to report to the Financial Intelligence Unit (UIF-Perú) arise under Ley N.° 27693 and Ley N.° 29038, as amended, which list mining companies among the persons required to report; under the rules of the Superintendencia de Banca, Seguros y AFP that define that category, a mining company is a reporting entity where, in addition to carrying on mining activity under a concession, it commercialises gold. This policy requires the compliance function to determine, on legal advice, whether and when a Peruvian Group company falls within that category.

9.2.2 International Standards and Frameworks

(a) FATF Recommendations: International standards on combating money laundering and the financing of terrorism and proliferation.

"Xstreco's policies set the standards that govern how the Group conducts its activities and how that conduct is assessed."

Xstreco AG
General-Guisan-Strasse 6
CH-6300 Zug
Switzerland

Email info@xstreco.com
Web xstreco.com