Fraud Policy

Group policy

xstreco

Contents

1 Introduction

1.1 Purpose and Scope

2 Policy Statement

2.1 Group's Stance on Fraud

2.2 Legal Implications

3 Key Principles and Guidelines

3.1 Specific Principles or Guidelines

3.2 Examples and Applications

4 Roles and Responsibilities

4.1 The Board

4.2 Executive Management

4.3 Responsibility for This Policy

4.4 Those Who Direct the Work of Others

4.5 Everyone Subject to This Policy

4.6 Counterparties

4.7 Those Responsible for Finance and Payments

5 Reporting and Monitoring

5.1 Reporting Mechanisms

5.2 Monitoring Procedures

6 Training and Awareness

6.1 Awareness on Appointment

6.2 Continuing Awareness

7 Compliance and Consequences

7.1 Reporting Non-Compliance

7.2 Consequences of Non-Compliance

8 Review and Revision

8.1 Review Frequency

8.2 Revision History

9 Appendices

9.1 Glossary of Terms

9.2 Related Legislation

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 the requirements that apply to the prevention, detection, investigation and reporting of fraud across the Group, and what is required of those subject to it where fraud is suspected.

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 Fraud

Fraud is prohibited. Engaging in, condoning or knowingly assisting a fraudulent act is prohibited, as is concealing one. Fraud exposes the Group and the individuals concerned to criminal and civil liability. This policy requires internal controls designed to prevent and detect fraud, routes through which concerns can be raised without retaliation, the prompt assessment and, where warranted, investigation of suspected fraud, and the remediation of fraud that is established.

2.2 Legal Implications

Article 146 of the Swiss Criminal Code makes fraud an offence, Article 152 false statements about a commercial business, Article 158 criminal mismanagement and Article 251 forgery of a document, which covers the false recording of accounting entries. Article 102 paragraph 1 makes the undertaking itself liable where inadequate organisation prevents the attribution of an offence to an individual. In Peru, fraud, fraudulent administration of a legal person and forgery are offences under the Código Penal. Ley N.° 30424, as amended, attributes administrative liability to legal persons for the offences in its catalogue, which does not include fraud as such. The policy takes account of the following standards and frameworks, which are not binding law:

(a) ISO 37001 (Anti-Bribery Management Systems): Requirements for an anti-bribery management system.

(b) ISO 37002 (Whistleblowing Management Systems): Guidance on whistleblowing management systems.

(c) COSO Fraud Risk Management Guide, Second Edition: Guidance on fraud risk governance, published jointly by COSO and the Association of Certified Fraud Examiners.

(d) OECD Guidelines for Multinational Enterprises on Responsible Business Conduct: Recommendations to enterprises, including on integrity and disclosure.

Non-compliance with this policy, and the conduct it prohibits, may result in reputational damage, internal disciplinary action, civil liability and criminal prosecution.

3 Key Principles and Guidelines

3.1 Specific Principles or Guidelines

This policy requires the following principles to be applied:

(a) Fraud Prevention: Internal controls, separation of duties, approval workflows and authorisation limits set by executive management must be established and applied, proportionate to the volume and the value of the transactions actually made.

(b) Fraud Detection: Review of transactions, independent checking of records and concerns raised under this policy must be used to identify red flags. Each Group company is subject to the audit that the law applicable to it requires. Where the scale of the Group's activities makes a further independent review of controls appropriate, this policy requires that one be commissioned.

(c) Fraud Response: A report of suspected fraud must be assessed promptly and, where it requires investigation, investigated, with confidentiality maintained except where disclosure is required by law or is necessary for the investigation, and then only to the extent necessary. Fraud that is established must be addressed through disciplinary action and, where appropriate, legal proceedings.

(d) Integration with Other Policies: This policy operates with the Anti-Corruption and Bribery Policy, the Whistleblowing and Ethics Reporting Policy and the Conflict of Interest Policy.

3.2 Examples and Applications

(a) Misappropriation of Group Assets: An employee uses Group funds to pay personal travel expenses. This is fraud and must be reported.

(b) Falsification of Records: A person alters a project cost record or a contractor invoice approval to conceal an unauthorised payment. This is fraud and must be reported.

(c) Contractor and Vendor Fraud: A person responsible for engaging a drilling or field services contractor arranges for invoice amounts to be inflated in exchange for a personal benefit. This is fraud and must be reported.

(d) Payroll and Personnel Fraud: A person with authority over field crew records claims payment for workers who did not attend site. This is fraud and must be reported.

(e) Expense Reimbursement Fraud: An employee submits duplicate receipts to claim more than the expense actually incurred. This is fraud and must be reported.

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 Finance and Payments

Those responsible for the Group's finances and for authorising payments are responsible for the separation of duties and the authorisation limits this policy requires, and for referring to the compliance function any transaction, record or entry that cannot be explained.

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 a fraud risk assessment be carried out and recorded, and be repeated 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 fraud, 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) Fraud: Deception intended to obtain an unlawful advantage or to cause loss to another.

(b) Internal Controls: The procedures and checks designed to prevent and detect fraud.

(c) Red Flags: Indicators of potential fraudulent activity.

(d) Misappropriation: The theft or misuse of Group assets.

(e) Fraud Risk Assessment: The identification and evaluation of fraud risk across the Group.

9.2 Related Legislation

9.2.1 Local Legislation

In Switzerland, Articles 146, 152, 158 and 251 of the Criminal Code (fraud, false statements about a commercial business, criminal mismanagement and forgery of a document, which covers the false recording of accounting entries) and Article 102 paragraph 1 of that Code (liability of the undertaking). In Peru, the Código Penal (fraud, fraudulent administration of a legal person and forgery) and Ley N.° 30424, as amended, which attributes administrative liability to legal persons for a defined catalogue of offences.

9.2.2 International Standards and Frameworks

(a) ISO 37001:2025: Requirements for an anti-bribery management system.

(b) ISO 37002:2021: Guidance on whistleblowing management systems.

(c) COSO Fraud Risk Management Guide, Second Edition (2023): Guidance on fraud risk governance, published jointly by COSO and the Association of Certified Fraud Examiners.

(d) OECD Guidelines for Multinational Enterprises on Responsible Business Conduct: Recommendations to enterprises, including on integrity and disclosure.

"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