Corporate Communications 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 who may communicate on behalf of the Group, how its external communications are approved and issued, and the standards those communications must meet. It covers media engagement, social media, crisis communication and communications with providers of finance, counterparties, communities and public authorities.

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 Corporate Communications

Public statements, public disclosures and media interactions must be accurate and must not mislead. Only authorised spokespersons may represent the Group in public or media engagements. Misleading and manipulative communications are prohibited, as is the presentation of a personal view as a position of the Group. Communications on political or public policy matters must be approved, before they are made, by a person designated for the purpose by executive management, must be consistent with the Political Engagement Policy, and, where they are made to public officials, must be authorised under that policy. Information given to providers of finance, counterparties and other external parties must be consistent with the information held internally and, where it is confidential, must be given only under an obligation of confidence.

2.2 Legal Implications

Article 3 paragraph 1 letter b of the Federal Act against Unfair Competition (SR 241) prohibits incorrect or misleading statements by an undertaking about itself, its business name, its goods, its services or its business circumstances, and Article 23 makes an intentional breach an offence prosecuted on complaint. The Federal Act on Data Protection and, in Peru, Ley N.° 29733, Ley de Protección de Datos Personales, apply where a communication contains personal data; see the Information Governance and Security Policy. In Peru, the Reglamento de Participación Ciudadana en el Subsector Minero, approved by Decreto Supremo N.° 028-2008-EM, governs the information given to the population in the area of influence of a mining activity, and communications with those communities must comply with it. The following are standards and frameworks rather than binding law:

(a) OECD Guidelines for Multinational Enterprises on Responsible Business Conduct: Recommendations addressed to enterprises, including on disclosure and stakeholder engagement.

(b) UN Global Compact: The ten principles on human rights, labour, the environment and anti-corruption.

(c) Transparency International Business Principles for Countering Bribery: Guidance for enterprises on countering bribery.

Non-compliance with this policy, and the conduct it prohibits, may result in reputational damage, legal penalties, and internal disciplinary action.

3 Key Principles and Guidelines

3.1 Specific Principles or Guidelines

This policy requires the following principles to be applied:

(a) Authorised Spokespersons: Only individuals designated by executive management may speak on behalf of the Group in public or media engagements. This policy requires that the designation be recorded, be kept current and be made known to those subject to this policy.

(b) Media Engagement: Media enquiries must be directed to those responsible for corporate communications. A press release or an interview requires prior approval from executive management, taking legal advice where the subject calls for it.

(c) Social Media Governance: Posting confidential or misleading information about the Group on social media is prohibited. A personal view must be clearly distinguished from a position of the Group.

(d) Crisis Communication: This policy requires executive management to designate the individuals who may issue public statements in a crisis, and requires that the designation be recorded, be kept current and be made known to those subject to this policy. In a crisis, only those individuals may issue public statements.

(e) Accuracy of Public Statements: A public statement must be accurate and must not mislead by act or omission, and must comply with the law applicable to it and with the confidentiality obligations the Group owes to providers of finance, counterparties and public authorities. Where the Group becomes subject to a statutory or contractual disclosure regime, a public statement must also comply with that regime.

(f) Stakeholder Engagement: Communication with stakeholders must be open, respectful and culturally sensitive.

3.2 Examples and Applications

(a) Unauthorised Public Statement: An employee gives an interview to a journalist without approval. This is a breach of this policy and must be reported.

(b) Press Release Issued Without Review: A press release is published without the approval this policy requires. This is a breach of this policy and must be reported.

(c) Social Media Misrepresentation: An employee posts misleading information about the Group or its activities on a social media platform. This is a breach of this policy and must be reported.

(d) Crisis Miscommunication: During an operational incident, an employee who is not designated under section 3.1 to issue public statements in a crisis shares unverified information online. This is a breach of this policy 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 Corporate Communications

Those responsible for the Group's external communications are responsible for obtaining the approval this policy requires before a statement is made publicly, for keeping a record of what was issued, by whom it was approved and on what basis, and for correcting a statement found to be inaccurate.

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) Authorised Spokesperson: An individual designated to speak on behalf of the Group in public or media engagements.

(b) Media Engagement: The process of interacting with media outlets to communicate information about the Group.

(c) Public Disclosure: The making of information available to the public, whether by statement, publication or response to an enquiry.

(d) Social Media Governance: The management of social media activity so that it is consistent with the values and policies of the Group.

(e) Crisis Communication: The management of communications during a crisis so that the information issued is accurate and authorised.

(f) Stakeholder Engagement: The process of engaging with stakeholders to address their concerns and interests.

9.2 Related Legislation

9.2.1 Local Legislation

In Switzerland, the Federal Act against Unfair Competition (SR 241), in particular Article 3 paragraph 1 letter b on incorrect and misleading statements by an undertaking about itself and its business circumstances and Article 23 on the criminal consequences, and the Federal Act on Data Protection (SR 235.1) where a communication contains personal data. In Peru, the Reglamento de Participación Ciudadana en el Subsector Minero, approved by Decreto Supremo N.° 028-2008-EM and implemented by Resolución Ministerial N.° 304-2008-MEM/DM, which governs information given to, and consultation with, the population in the area of influence of a mining activity, and Ley N.° 29733, Ley de Protección de Datos Personales, where a communication contains personal data.

9.2.2 International Standards and Frameworks

(a) OECD Guidelines for Multinational Enterprises on Responsible Business Conduct: Recommendations addressed to enterprises, including on disclosure and stakeholder engagement.

(b) UN Global Compact: The ten principles on human rights, labour, the environment and anti-corruption.

(c) Transparency International Business Principles for Countering Bribery: Guidance for enterprises on countering bribery.

> “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