Information Governance and Security 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 the requirements that apply to the classification, protection, retention and destruction of the information of the Group at each stage of the data lifecycle. It covers personal data, intellectual property and commercially sensitive information, and applies to that information in whatever form it is held.

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 Information Governance and Security

Information must be managed and protected according to its sensitivity, its commercial value and the legal obligations attaching to it. Information must be classified so that ownership, access rights and protection measures can be set for each class, and handled so as to preserve its confidentiality, its integrity and its availability. Disclosure outside the Group of information that is not intended for external use is prohibited unless it is authorised under this policy or the Corporate Communications Policy, is made in the ordinary course of the Group's business to a person who needs it, is required by law, or is a concern raised through the channels in section 5.1 or with a competent authority.

2.2 Legal Implications

The Federal Act on Data Protection (FADP, SR 235.1) and the Data Protection Ordinance (SR 235.11) govern the processing of personal data by the Group in Switzerland and any processing, wherever carried out, that has an effect in Switzerland. In Peru, Ley N.° 29733 and its reglamento govern processing carried out there. Regulation (EU) 2016/679 (GDPR) applies to the Group only where personal data are processed in the context of an establishment in the European Union, or where goods or services are offered to people in the European Union, or their behaviour in the Union is monitored. ISO/IEC 27001, ISO/IEC 27701 and the NIST Cybersecurity Framework are standards and frameworks rather than binding law; they bind the Group only where a contract or a financing agreement so requires. 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) Data Classification and Labelling: Information must be classified according to its sensitivity and business impact, and labelled accordingly.

(b) Access Control and Least Privilege: Access to information must be granted according to role and business need, and reviewed on a defined cycle.

(c) Data Retention and Secure Destruction: Information must be retained for the period the law applicable to it requires and, subject to that period, only as long as it is needed, and securely destroyed once it is not.

(d) Encryption and Secure Transmission: Information classified as sensitive must be protected in transit and at rest by encryption or by another control appropriate to its sensitivity and to the systems in which it is held, using recognised protocols, and the control chosen must be recorded.

(e) Incident Response and Breach Notification: An incident response plan covering cybersecurity incidents and data breaches must be established, kept current and tested, and a data breach must be notified where the applicable law requires it.

(f) Rights of Individuals: A request from an individual to exercise a right under the applicable data protection law must be recognised, recorded and passed without delay to the compliance function, which assesses it and responds within the period the applicable law allows.

(g) Third-Party Risk Management: Suppliers and counterparties that hold or have access to the Group's information must be assessed against the information security standards in this policy, on a risk basis proportionate to the information concerned. Where personal data are entrusted to them, the processing must be governed by a written agreement meeting the requirements of the applicable data protection law, made before the data are disclosed to them.

(h) Cross-Border Transfers of Personal Data: Personal data must not be transferred to another country, whether to a third party or within the Group, unless the conditions the applicable data protection law sets for that transfer are met.

3.2 Examples and Applications

(a) Handling a Data Breach: A system is compromised, exposing personal data. The incident must be reported and investigated and, where the applicable data protection law so requires, notified.

(b) Managing Access to Sensitive Information: An employee leaves the Group. Their access to internal systems must be revoked on departure so that unauthorised access is prevented, and the revocation must be recorded.

(c) Responding to Phishing Attempts: An employee receives a suspicious email. It must be reported to those responsible for information systems, who assess it and respond to it.

(d) Unauthorised Cloud Storage: An employee stores sensitive files on an unapproved cloud service. This must be reported and addressed through enforcement of this policy and training.

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 Information Systems

Those responsible for the Group's information systems are responsible for the access controls, the retention arrangements and the response to an incident that this policy requires, and for keeping the records from which compliance can be shown. The means used are proportionate to the systems and the data actually held.

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) Data Breach: A breach of security leading to the accidental or unlawful loss, destruction or alteration of information, or to its disclosure to, or access by, a person not authorised to receive it or to access it.

(b) Encryption: The process of converting information into a secure format that can only be read by authorised individuals.

(c) Access Control: Measures by which access to sensitive information is restricted to authorised personnel.

(d) Personal Data: Any information relating to an identified or identifiable natural person.

(e) Information Governance: The management of information so as to preserve its availability, integrity and confidentiality.

(f) Cybersecurity Incident: An event that threatens the security of information systems or of the information they hold.

(g) Data Lifecycle: The stages through which data passes, from creation and use to storage and destruction.

9.2 Related Legislation

9.2.1 Local Legislation

In Switzerland, the Federal Act on Data Protection (FADP, SR 235.1) and the Data Protection Ordinance (SR 235.11). In Peru, Ley N.° 29733, Ley de Protección de Datos Personales, and its reglamento, approved by Decreto Supremo N.° 016-2024-JUS.

9.2.2 International Standards and Frameworks

(a) ISO/IEC 27001:2022: Requirements for an information security management system, with Amendment 1:2024.

(b) NIST Cybersecurity Framework 2.0 (2024): Voluntary guidance on managing cybersecurity risk.

(c) Regulation (EU) 2016/679 (GDPR): Binding law within its scope; it applies to the Group to the extent set out in section 2.2.

(d) ISO/IEC 27701:2025: Requirements and guidance for a privacy information management system; since the 2025 edition an independent management system standard.

"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