Security Policy

04-2026

Alstom faces evolving threats in a crisis-driven geopolitical environment marked by renewed economic and strategic competition. Traditional threats such as terrorism, organised crime and armed conflicts are intensifying, and are compounded by new, sometimes hybrid, forms of attack, including cyber attacks, espionage and disinformation campaigns.

Alstom must adapt its analyses and responses to ensure the company's robustness and development, anticipating security disruptions in a cross-functional approach to counter any malicious actions directed against it.

Alstom constantly commits to **new fields of activity**, using new tools, both industrial and digital, and **diversifying its geographical footprint**. Therefore it evolves in a complex and sometimes dangerous environment, increasingly facing new security risks.

Today, consideration of these risks **fundamentally conditions** our collective ability to **exploit opportunities**, to successfully **conduct our operations** and to efficiently **deliver to our customers**.

Security encompasses all active and passive measures allowing Alstom to **anticipate, prevent, protect** itself against and **react** to any kind of intentionally malicious action, both in material and immaterial fields.

As expressed by Martin Sion in the Sustainability and Corporate Social Responsibility policy, the implementation of a Security policy, based on proven processes, **known by all** and **applied by each**, will allow us to increase our **resilience**, assert our **competitiveness** and **strengthen our leading position**.

Christophe Caussin

Chief Security Officer

Our commitments

- To implement the necessary measures to ensure the highest possible level of security for **all Alstom** employees, wherever they are in the world;
- To guarantee, to the best of our ability, the integrity of **our sites and our projects**;
- To ensure our **ability to deliver** our products and services;
- To protect our **information**, our **know-how** and our **reputation**;
- To make all the measures and actions taken in the security field compliant with the **Alstom Code of Ethics**, the **domestic laws** from the countries we work in and the **international law**.

The principles behind our stategy

- **To consider the threat as a whole**:
  - Build a transverse understanding of security issues consequences;
  - Integrate security natively into our processes;
  - Provide adapted, consistent and coordinated responses;
  - Take into account all stakes, including cybersecurity issues by enforcing Alstom Information Security Model at every relevant level.
- **To think our actions in a proactive way:**
  - Establish and update our own threat assessments;
  - Include security topics as far upstream in operations and projects as possible;
  - Implement an active policy of lessons learned.
- **To make each and every employee responsible for the company global security:**
  - Reinforce awareness as well as individual and collective behaviours;
  - Inform and train our employees;
  - Develop a Security culture.

ALS-POL-005 V6