Security Policy

To be used as is

Approved By :	Christophe CAUSSIN/ Chief Security Officer	22/03/21

SECURITY POLICY

03-2021

Alstom is continuously exposed to a growing number of threats with increasingly serious consequences: geopolitical unrest, terrorism, organised crime, cybercriminality, information theft, economic instability, and many others. Taking malicious actions against Alstom into account is today a prerequisite of our company's existence and development.

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, regularly facing new security risks.

Today, consideration of these risks **fundamentally conditions** our collective ability to smoothly grow up, to effectively protect our innovations, and to efficiently deliver to our customers.

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

As expressed by Henri Poupart-Lafarge 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 **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 STRATEGY

- **To consider the threat as a whole, so as to elaborate robust, comprehensive and consistent action plans:**

Consider the security implications of every one of Alstom's people and fields of activity, taking 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, aiming for anticipation and prevention as much as effective reaction:**

Establish our own internal assessments, keeping them up to date; include security issues as far upstream in projects as possible; adapt ourselves by implementing an active policy of lessons learned.

- **To make each and every person responsible for the company global security, feeling involved whatever their field and level:**

Reinforce awareness and the codes of individual and collective behaviour for both employees and subcontractors.

ALSTOM
• mobility by nature •

ALS-POL-005-VD_EN