



Atos Security Policy Statement

Atos Group is a global leader in the Digital realm and is committed to best protect its assets from all threats and to deliver reliable and secure products and services, pursuing these goals through constant innovation.

**Perimeter**


- ▶ Atos Group security policies apply to all employees, contractors, and temporary staff, covering all forms of information (electronic, paper, discussion, etc.), whether owned by, held in custody for customers or used by Atos Group.
- ▶ In such context, the safety and physical security (people and sites) domains are essential, and both contribute to enforcing the protection of Atos Group and customers assets.


**Objectives**


- ▶ The Atos Group security policies of the company aim to ensure that:
 - ✓ Information will be protected against unauthorized access, notably through Multi Factor authentication for all internal applications.
 - ✓ Confidentiality of information will be assured; Integrity of information will be maintained and Availability of information preserved.
 - ✓ Classification of information will be applied.
 - ✓ Security and privacy risk assessments will be performed by security officers and data protection officers with asset owners to identify and evaluate security and privacy risks so that appropriate preventative measures can be taken. This will be performed in accordance with EU GDPR regulations.
 - ✓ Identified high and medium security vulnerabilities will be remediate by operations without any delay.
 - ✓ Country regulatory, legislative, and contractual security-related requirements will be met.
 - ✓ All staff will undergo regular security awareness training.

**Roles and Responsibilities**


- ▶ The Group CISO is responsible for ensuring the organization of security within Atos Group. He is directly responsible for updating this security policy and the yearly security targets as well as providing advice and assistance on its implementation. For this mission, he relies on a dedicated Strategic Function organization.
- ▶ All staff are the first line of defense in security, their support and adherence to security policies are essential and mandatory.
- ▶ All managers are directly responsible for implementing the Security Controls defined by Policies within their business areas and for adherence by their staff.
- ▶ Staff should immediately report all breaches of security and security incidents to their closest security officer or failing that to their manager.
- ▶ In the event of a security incident, immediate action must be taken to mitigate the risk and impact of damage to Atos Group and its customers.
- ▶ Exceptions to the Atos Group security policies require the approval of the Group CISO.
- ▶ It is the responsibility of all members of staff to adhere to the Atos security policies and related standards, procedures and guidelines including Aide-Mémoire principles. Breach of these documents may result in disciplinary action, up to and including termination of employment.

**Atos Group security management system**

- ▶ To achieve its security goals in protection of information, Atos has developed an information security management system (ISMS) based on ISO 27001 standard which is mandatory for all Atos business activities worldwide.
- ▶ Additional standards, procedures, and guidelines to the global policies must be produced locally to support the local implementation of the global policies in accordance with local legislation. These local rules define the minimum level of compliance for all employees regarding security.
- ▶ More information on Atos SharePoint: atos365.sharepoint.com > Home  > Support Functions > Security



Approved by:
Philippe Salle
Chairman and CEO, Atos Group



Approved by:
Paul Bayle
Group Chief Information Security Officer