Atos Security Policy Statement

Atos Group is a global leader in the Digital realm and is committed to protect its assets from 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 (including but not restricted to electronic information and paper), whether owned by or held in custody for customers, or used by the Group.
- In such context, domains pertaining to the safety and physical security of people and sites are essential. Both contribute to enforcing the protection of the Group and customers' assets.

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 global policies must be produced locally to support the local implementation of the aforesaid policies in accordance with local legislation. These local rules define the minimum level of compliance for all employees regarding security.
- For more information, refer to the Atos SharePoint: atos365.sharepoint.com > Home > Support Functions > Security

Roles and Responsibilities

- The Group CISO is responsible for ensuring the organization of security within the 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 members of 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 security breaches 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.
- Any exception to the Atos Group security policies requires 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.

Objectives

The Atos Group security policies aim to ensure the following:

- Information will be protected against unauthorized access, notably through multifactor authentication (MFA) 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. Following this, appropriate preventative measures will be taken in accordance with EU GDPR regulations.
- Any identified high and medium security vulnerabilities will be immediately remediated by the operations team.
- Country regulatory, legislative, and contractual security-related requirements will be met.
- All staff will undergo regular security awareness training.

106571 - JS + GR