Atos Security Policy Statement

Atos is a global leader in the digital realm, committed to protecting its own assets against all threats and to delivering reliable, secure products and services through continuous innovation. In the course of its activities, Atos pays particular attention to the protection of client assets entrusted to the Group, ensuring appropriate governance and providing advisory and compliance mechanisms—always in accordance with contractual agreements and the specific expectations of each client.

Perimeter

- Atos Group security policies apply to all employees, contractors, and temporary staff, covering all forms of information (electronic, paper, discussion, etc.) that are owned by Atos, used by Atos, or entrusted to Atos by its clients.
- Atos Group Security holds a global mandate and is governed centrally. Security rules and standards — including cybersecurity, physical security, health, and safety — are strictly mandatory and uniformly applied across all geographies and business lines, with no exceptions.
- For client assets entrusted to Atos, protection measures are implemented strictly according to contractual agreements and client requirements, with particular attention to respecting ownership and risk assessment responsibilities.
- Safety and physical security, covering people (wherever applicable) and sites, are essential and contribute to the protection of both Atos Group and client assets.

Atos Group security management system

- All staff receive regular security awareness training.
- Atos has established an information security management system (ISMS) based on ISO 27001 standard which is mandatory for all Atos business activities worldwide.
- Governance and operational controls for clients are supported by roles, such as Client Delivery Executives accountable for their client's security and Client Security Managers operationally responsible for security, with a mission to facilitate compliance and provide expert guidance to clients and account teams.
- Local standards and procedures are developed to support global policies, ensuring compliance with local laws and defining minimum security requirements for all employees.
- More information on Atos SharePoint: atos365.sharepoint.com > Home > Support Functions > Security

Roles and Responsibilities

- The Group Chief Information Security Officer (CISO) is responsible for organizing security within Atos Group, updating the security policy, and setting annual security objectives. For this mission, he relies on a dedicated Support Function organization.
- All staff are the first line of defense and must comply with security policies and procedures.
- It is the responsibility of all members of staff to adhere to 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.
- Managers are responsible for implementing security controls within their areas and ensuring their teams adhere to the Atos policies.
- Security officers, Client Security Managers and data protection officers conduct and document risk assessments in collaboration with asset owners and clients (internals or externals) and manage exceptions.
- For client assets entrusted to Atos, Client Security Managers are responsible for implementing governance and compliance measures as defined by contractual agreements and client requirements.
- All security incidents and breaches must be reported immediately to the appropriate security officer or manager, and appropriate actions must be taken to mitigate risks and impacts to Atos and its clients.

Objectives

- Information is protected against unauthorized access, notably through Multifactor authentication.
- Confidentiality, integrity, and availability of information are maintained.
- Information is classified appropriately.
- Security and privacy risk assessments are performed by security officers and data protection officers, together with asset owners, to identify and evaluate security and privacy risks so that appropriate preventative measures can be taken. These assessments are conducted in accordance with applicable regulations (e.g. EU GDPR) and relevant contractual obligations.
- Operational security risks are documented and managed
- Critical and high security vulnerabilities are remediated without delay.
- Regulatory, legislative, and contractual security requirements are met

Approved by:

Philippe Salle
Chairman and CEO, Atos Group

Approved by:

Paul Bayle
Group Chief Information Security Officer

107386-JS+GR-Poster-Atos security