



INFORMATION SECURITY POLICY

LEONARDO TURKEY AVIATION, DEFENSE AND SECURITY SYSTEMS INC. adopts the protection of the confidentiality, integrity, and availability of information assets as one of its primary priorities while conducting its activities. In this context, an effective and sustainable Information Security Management System (ISMS) has been established and implemented in accordance with the ISO/IEC 27001 standard and the requirements of EASA Part-IS.

Our organization is committed to systematically identifying, assessing, and managing information security risks; complying with legal, regulatory, and contractual requirements; and raising the information security awareness of employees and business partners. Information security management is not limited to technical measures, but also encompasses process, human, and organizational dimensions. This Information Security Policy has been approved by top management and is mandatory for all employees, contractors, and business partners.

To plan and carry out all information security activities in a manner that supports business continuity and enhances resilience against cyber threats,

To manage processes such as access control, backup, network and system security, incident management, business continuity, and disaster recovery through an integrated approach,

In information security risk assessments, not only the impacts on information assets but also the potential impacts of risks on aviation safety shall be taken into account.

To regularly review the effectiveness of the Information Security Policy and update it in line with evolving needs, technological innovations, and regulatory requirements,

To ensure that top management guarantees the continual improvement of the information security management system, the allocation of necessary resources, and the achievement of policy objectives,

This is the Information Security Policy of Leonardo Turkey.

Leonardo Turkey

Paolo SEBASTIANI

General Manager