INFORMATION SECURITY POLICY

1. Purpose, Scope, and Objectives of Information Security

As CES. Advanced Composites and Defense Technologies Inc., we aim to ensure information security in compliance with the requirements of the ISO 27001 Information Security Management System standard. This includes customs and foreign trade activities such as import, export, transit, and customs clearance related to polymer matrix composite products for the defense, aerospace, space, automotive, rail systems, and ballistic industries, as well as supporting functions including logistics, warehousing, accounting, finance, and information technologies, together with the electronic information assets used in these activities and the cybersecurity measures implemented to protect them.

Our company defines and implements security standards and practices related to the information technology infrastructure and access to the networks in use.

- Is responsible for ensuring the confidentiality, security, integrity, and availability of all data shared within information systems.
- Aims to ensure business continuity and minimize legal risks that may arise from security breaches.
- Is responsible for maintaining the credibility and reputation of the organization.
- Ensures compliance with Law No. 5651, the Law on Intellectual and Artistic Works, Law No. 6698 on the Protection of Personal Data (KVKK), and the resolutions of the Board of Directors within the scope of information security.
- Ensures information security in line with risk analysis outcomes.
- Reports information security incidents to the Information Security Management Representative to enable necessary actions to be taken.
- Carries out continuous improvements to meet the requirements of the Information Security Management System.
- Protects the confidentiality, integrity, and availability of information belonging to relevant interested parties.
- Due to legal obligations, all accesses originating from the CES network are logged and retained for the period and detail specified by applicable legislation.

To ensure that information is understood by employees and remains up to date:

- Aims to conduct trainings to increase information security awareness.
- Aims to ensure the continuity of the Information Security Management System.

2. Employee Participation and Responsibilities

The purpose of the Information Security Management System and this policy is to protect, maintain, and manage the confidentiality, security, integrity, and availability of all information. All CES employees, outsourced personnel, business partners, and interns are responsible for ensuring the protection of information within CES in accordance with their roles and positions. CES personnel are required to comply with the principles of the ISO 27001 Information Security Management System, the protection of confidential information defined under Facility Security requirements, and the CES Code of Ethics.
CES is committed to taking the necessary measures and ensuring full compliance with Law No. 5651 on the Regulation of Publications on the Internet and Combating Crimes Committed Through Such Publications, the Law on Intellectual and Artistic Works, and Law No. 6698 on the Protection of Personal Data.

3. Measures, Commitments, and Responsibilities Regarding Data Security

Each department manager is primarily responsible for taking the necessary measures to ensure compliance with the Information Security Policy and for overseeing the effectiveness of the system. Top Management shall ensure that all employees receive appropriate training to enhance information security awareness. Top Management is also responsible for ensuring that the requirements of this policy are communicated to all employees and contractor personnel. Employees are responsible for being aware of the Information Security Policy and complying with its principles.

Our Information Security Policy is aligned with the Açık Holding Code of Business Ethics and the Açık Holding Information Security Policy.

General Manager
MURAT GİRAY