SECURITY POLICY

1.- INTRODUCTION

Aernnova is specialized in the design, manufacture, and maintenance of advanced technology aerostructures, as well as the components, systems and equipment related to them, contributing with this Mission to connect people and to economic and social development.

The Board of Directors of Aernnova Aerospace Corporation has approved this Security Policy.

.2- SUBJECT

The purpose of this policy is to establish a general framework of reference for the protection of personnel, information and technology resources associated with it and Aernnova's assets. Security measures at Aernnova are aimed at:

• protect personnel, activities and valuable assets (information, technological assets, facilities and reputation) against any hostile act that could compromise their security.

• preserve our staff’s privacy and the confidentiality of our customers.

• prevent, detect and respond to any hostile act, accidental or intentional, against personnel, activities and valuable assets.

3- FUNDAMENTALS

• The required security levels will be based on the risk analysis performed by Aernnova.

• All Aernnova personnel must comply with this Policy and related internal documentation and regulations.

• The requirements derived from this Policy shall be contractually binding on associated third parties.

• Corporate assets and confidential or restricted information shall be protected against all forms of access, use, copying, disclosure, modification, and destruction.

Responsibilities

Achieving an adequate level of security requires the participation of the entire Aernnova organization:

1. Personnel responsibilities

Aernnova personnel must observe the security requirements, regulations, and internal procedures.

Each professional must take due care of his or her own workspace, tools, equipment, technological resources and information and data resources (hereinafter, assets) as provided by Aernnova, our Customers and Suppliers, for the performance of his or her professional duties.

All personnel shall ensure that these assets are properly turned over when they are no longer needed.

2. Responsibilities of the Security Committee

The Security Committee will be responsible for ensuring the implementation and maintenance of Aernnova's Security Management System. This includes overseeing the correct application of security regulations, and providing consulting assistance in:

• policy, manuals, directives, standards, procedures and guidelines for interpretation and enforcement

• technical and procedural execution,

• communications,

• conducting audits and reviews for compliance with policies and risk assessments.

The Security Committee shall ensure that global or local policies or procedures are consistent with the requirements of this policy.

3. Responsibilities of third parties

The personnel of contractors and subcontractors shall be responsible for observing these rules when accessing Aernnova facilities, assets, and information.

To this end, Aernnova's security directives shall be communicated to third parties and, if necessary, added as an annex to the corresponding contractual documentation.

Security principles

The following principles will be applied in specific directives, procedures, standards and guidelines.

1. Access controls

Physical security will be managed through access control systems that ensure safe and regulated entry to the facilities. Access to buildings will be managed through a combination of technological and procedural controls, ensuring that only authorized personnel and visitors enter, while maintaining a secure environment that protects our staff, assets, and information.

Visitor management and staff access will be governed by clear directives and protocols, ensuring that access is granted based on the requirements of the visitor's role and purpose, and will be subject to regular reviews and audits to ensure ongoing security and compliance with regulatory standards.

2. Physical and operational security

Access to all the company's protected assets shall be recorded and monitored in accordance with local regulations, observing the procedures defined for this purpose.

Rigorous guidelines and training for security personnel will be implemented, ensuring minimal and proportionate use of force, respecting freedom of movement and maintaining transparency, accountability, and respect for individual rights in all security operations.

3. Business travel and foreign assignments

Appropriate care, assistance and advice should be assured for personnel traveling and/or working abroad as they may be exposed to security risks in some countries or locations.

4. Information and Communication Technology (ICT) Systems

Aernnova is committed to ensuring the security of our IT systems while prioritizing user privacy, data integrity and system availability, adhering to the highest ethical and legal standards in all digital interactions and controls.

We aim to maintain transparency in our digital practices and apply them in a way that maintains optimal functionality and accessibility, with the goal of safeguarding system and data integrity without compromising them.

5. Information Control

A robust information security framework must be developed and maintained to ensure that authorized individuals have accurate access to the information they need, while diligently preventing unauthorized access.

By implementing robust controls, we will protect the integrity and availability of information and align our practices with a comprehensive approach that prioritizes confidentiality, resilience to cyber threats and regulatory compliance.

6. Disaster Recovery / Business Continuity

Events that can cause disruptions to business processes should be identified, along with the likelihood and impact of these disruptions and their consequences for information security.

Business continuity plans and procedures will be maintained, tested and updated to ensure the continuous availability of business processes.

7. Incident Management

A structured incident management process will be implemented to identify, respond to and mitigate security incidents in a timely and effective manner.

The process should include clear reporting channels, defined roles and responsibilities, and a systematic approach to incident analysis, documentation and communication to ensure that incidents are managed effectively and that lessons learned are incorporated into ongoing security practices.

4-. CONTROL SYSTEM

Aernnova's Management is responsible (within its scope) for ensuring the implementation and periodic review of this policy and the Security Management System defined in the Manual (MDG-00-401).The Control system includes, but is not limited to:

• Implementing an operational security system that ensures the protection of people and assets of the different entities that make up Aernnova.

• Establishing security policies and procedures for the information systems whose purpose is to protect the information in Aernnova's global network.

• Ensuring, through a security event reporting system, that all security-related information is reported and properly managed.

5- STAKEHOLDERS COMMUNICATION AND ENGAGEMENT

The Security Policy is targeted to all Stakeholders: Customers, Authorities, Shareholders, Employees, Suppliers, and Consumers and Society as a whole. It has been communicated and is understood within the scope of the organization and is available through the communication and information channels that the company makes available to all its stakeholders. It is publicly available on the Aernnova website.