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 for application to the above activities.

.2- SUBJECT

This Security Policy establishes the management principles and management's commitment to protect personnel, information and technology resources associated with it, and Aernnova's assets, as well as to preserve the safe operation of processes and products delivered and in service.

Security measures at Aernnova are aimed at:

•Protect personnel, activities and valuable assets (information,

technological assets, facilities and reputation) against any hostile act or vulnerability that could compromise their security or aviation 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 or aviation security.

• Satisfy applicable security and information security requirements: regulatory, contractual or other requirements to which the organization subscribes, considering industry standards and best practices, as well as social expectations.

• Provide a reference framework to establish objectives and measure the performance of information security and provide continuous improvement of the system to achieve higher levels of security.

Ed. 2 Rev. 2	17/07/2025	General Update
Ed. 2 Rev. 1	22/05/2025	General Update
Ed. 2 Rev. 0	12/06/2023	General Update
Ed. 1 Rev. 0	02/07/2018	First Edition

3- FUNDAMENTALS

• The required security levels shall consider the risk analysis performed by Aernnova, which shall be carried out periodically and in accordance with the applicable procedures.

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

• The requirements derived from this Policy shall extend to associated third parties.

• A security culture of transparency and open communication will be fostered, encouraging personnel to report any vulnerability, anomalous or suspicious event, or security incident in an atmosphere of trust and accountability. The principle of Just Culture, whereby individuals are not punished for actions, omissions or decisions made in accordance with their experience and training, will be respected at all times, but gross negligence, concealment, intentional violations, or destructive or unlawful acts will not be tolerated.

• Corporate assets and confidential or restricted information shall be protected against all forms of access, use, copying, disclosure, modification, and destruction, ensuring their confidentiality, integrity and availability, in accordance with applicable legal, contractual and regulatory requirements.

Responsibilities

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

1. Personnel responsibilities

A security culture will be fostered in the organization through training and security promotion communications.

Staff participation is key by observing 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.

Access to and use of these assets will cease when they are no longer needed.

Ed. 2 Rev. 2	17/07/2025	General Update
Ed. 2 Rev. 1	22/05/2025	General Update
Ed. 2 Rev. 0	12/06/2023	General Update
Ed. 1 Rev. 0	02/07/2018	First Edition

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 evaluation and continual improvement of this policy and the effectiveness of the security management system. They shall be evaluated annually or more frequently, if necessary, to adapt to changes in risks, regulations or the organizational environment.

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 onthe 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.

Ed. 2 Rev. 2	17/07/2025	General Update
Ed. 2 Rev. 1	22/05/2025	General Update
Ed. 2 Rev. 0	12/06/2023	General Update
Ed. 1 Rev. 0	02/07/2018	First Edition

2. Physical and Operational Security

Access to all protected company assets will be logged and monitored in accordance with local regulations, following defined procedures.

Rigorous guidelines and training will be applied to security personnel, ensuring the 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 Missions Abroad

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

4. Information Security

AERNNOVA is committed to ensuring the security of our IT systems while prioritizing the privacy of each individual, 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 aim of safeguarding the integrity of the system and data without compromising them.

5. Information Control

A robust information security framework is 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, cyberthreat resilience, and regulatory compliance.

Aernnova implement security controls to guarantee the confidentiality of information, ensuring that only authorized persons have access to sensitive data. The information will be protected throughout its life cycle and compliance with these measures by employees, suppliers and third parties will be ensured through confidentiality agreements and appropriate security measures.

6. Disaster Recovery / Business Continuity

Events that can cause disruptions to business processes must 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 continued availability of business processes.

Ed. 2 Rev. 2	17/07/2025	General Update
Ed. 2 Rev. 1	22/05/2025	General Update
Ed. 2 Rev. 0	12/06/2023	General Update
Ed. 1 Rev. 0	02/07/2018	First Edition

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, as well as for internal and external incident reporting.

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

All Aernnova managers are responsible (within their scope of action) for ensuring the implementation and periodic review of this policy and the Security Management System defined in the Manual (MDG-00-401) and for allocating the necessary resources for its compliance, including personnel, technology and infrastructure, and the necessary budget for the effective implementation and operation of the Information Security Management System (ISMS).

The competencies required for personnel involved in information security-related activities shall be determined and documented. These competencies shall be available and periodically assessed to ensure that personnel have adequate knowledge to fulfill their responsibilities.

The Control System includes, but is not limited to:

• The implementation of an operational security system described in MDG-00-401 and in the associated procedures, which ensures the protection of the people and assets of the different entities that make up Aernnova and the confidentiality, integrity and availability of the information in Aernnova's global network.

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

• Appropriate indicators shall be established to evaluate the effectiveness of the system and periodic objectives for continuous improvement.

• The control system includes the performance of internal audits to annually assess compliance with regulatory, contractual or other requirements to which the organization subscribes, as well as the effective implementation and maintenance of the ISMS.

Management regularly monitors the performance of the ISMS as established in the review of the System, ensuring that it is aligned with Aernnova's strategic objectives and fostering an organizational culture that values information security.

5- STAKEHOLDERS COMMUNICATION AND ENGAGEMENT

The Security Policy is addressed to all Stakeholders: Clients, Authorities, Shareholders, Aernnova Staff, Suppliers, Consumers, and Society as a whole. Aernnova recognizes the importance of identifying and understanding key stakeholders, both internal and external, that affect and are affected by its activities, as well as applicable laws, regulations, and contracts. Furthermore, Aernnova ensures compliance with applicable regulations related to information security, both locally and globally, and maintains a continuous process of reviewing and adjusting its practices and procedures to adapt to any legislative or regulatory changes. This ensures the ongoing protection of confidentiality, integrity, and availability of information.

Aernnova continuously identifies and assesses the expectations, specific information security requirements, and legal and contractual obligations of its stakeholders.

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 its stakeholders. It is publicly available on the AERNNOVA website.

Ed. 2 Rev. 2	17/07/2025	General Update
Ed. 2 Rev. 1	22/05/2025	General Update
Ed. 2 Rev. 0	12/06/2023	General Update
Ed. 1 Rev. 0	02/07/2018	First Edition