

	[Corporate Information Security Policy]	Section
		Rev [2.0]
	[IHFA_Cybersecurity]	[01/12/2025]
		Page 1 of 5

[IHFA_Cybersecurity]

[Confidential]

[Corporate Information Security Policy]

IACOBUCCI HF Aerospace SpA

Road SC ASI 1/S nos. 16-18 - 03013 Ferentino (FR) - ITALY
Tel: +39.0775.39251; Fax: +39.0775.390009 - www.iacobucci.aero

	[Corporate Information Security Policy]	Section
		Rev [2.0]
	[IHFA_Cybersecurity]	[01/12/2025]
		Page . 2 of 5

Revisions

Rev	Date	Causal	Publisher	Verify	Approval
1	18/11/2025	First Issue	Gyala	Iacobucci	Iacobucci
2	01/12/2025	Added control themes	Pyramis	Iacobucci	Board of Directors

Page changes

PAGE	REV.	DATE
All	2	01/12/2025

ALL.	REV.	DATE

	[Corporate Information Security Policy]	Section
		Rev [1]
	[IHFA_Cybersecurity]	[18/11/2025]
		Page 3 of 5

CORPORATE INFORMATION SECURITY POLICY (ISO/IEC 27001)

with reference to EU Directive 2022/2555 NIS2

Premise :

In Iacobucci HF Aerospace SpA we are specialized in:

“ Design and manufacturing of premium solutions for the aviation industry, creating Galley Inserts , VIP Seats and Trolleys both nationally and internationally, with a strong focus on quality and innovation .”

We understand the importance of maintaining high product quality standards and, above all, our credibility with our customers. Safeguarding the information that protects our expertise and that of our customers, suppliers, and all stakeholders is our duty. Therefore, we are fully aware of the importance of adequate security management, and we have therefore decided to implement an Information Security Management System (ISMS) compliant with ISO/IEC 27001:2022 to ensure the confidentiality, integrity, and availability of all the information we manage.

At Iacobucci HF Aerospace SpA, together with the collaboration of its staff, we have decided to establish and maintain an Information Security Policy compliant with the ISO/IEC 27001:2022 standard. This ensures greater control over security and risk management, consistent with the company's strategic objectives and maintaining the right balance between:

- the company's strategic plan and the policies and strategies of Customers and Suppliers;
- compliance with national and international regulations, including Directive 2022/2555 (NIS2 Directive), to ensure a systematic approach to information security management;
- the continuous improvement of the effectiveness and efficiency of our security processes and controls;
- constant adaptation to the context in which we work;
- the identification, assessment and mitigation of risks;
- optimizing business risk management to reduce potential financial losses and ensure operational resilience;
- Raising awareness of information security, security policies, and procedures, including internally, by ensuring ongoing and in-depth training for all employees.

By ensuring the ISMS's direct support in achieving long-term corporate goals, we firmly believe this will strengthen our corporate reputation while maintaining high standards of security and transparency. Furthermore, it will allow us to consolidate our competitive position in the market and offer customers and stakeholders greater confidence in the secure management of information.

	[Corporate Information Security Policy]	Section
		Rev [1]
	[IHFA_Cybersecurity]	[18/11/2025]
		Page 4 of 5

At Iacobucci HF Aerospace SpA we have decided to implement and maintain the ISMS in order to:

- implement a structured system for identifying, analyzing, and managing information security risks;
- implement a continuous process for identifying and addressing vulnerabilities, with the aim of promptly reducing attack surfaces and preventing potential cyber incidents;
- ensure accurate and up-to-date management of information assets, ensuring their traceability and proper maintenance throughout their life cycle;
- strengthen corporate network protection measures, through multi-layered defense solutions and effective controls on internal and external communications;
- Continuously monitor security events and system logs to promptly detect anomalous activities and ensure effective incident response.
- ensure that critical information is protected from internal and external threats, ensuring business continuity through Disaster Recovery and Business Plans Continuity;
- ensure adequate levels of physical security, protecting critical infrastructure from unauthorized access and environmental risks;
- manage the life cycle of IT systems and networks through structured procedures that ensure their safe installation, maintenance, updating, and decommissioning;
- constantly monitor the performance of the ISMS through specific key performance indicators, identifying areas for improvement;
- promote a safety-oriented corporate culture, with continuous staff training and awareness-raising activities;
- adopt periodic review processes to ensure that the ISMS remains aligned with regulatory, technological and organizational changes;
- facilitate legal and regulatory compliance through standardized operating procedures and regular internal audits;

At Iacobucci HF Aerospace SpA, we strive daily to ensure maximum information security, adopting a structured approach and involving every level of our organization. We firmly believe in the importance of ensuring that everyone, from our employees to external collaborators and business partners, strictly adheres to the security requirements we have established.

For us, regulatory compliance is not just a formal obligation, but a fundamental value.

	[Corporate Information Security Policy]	Section
		Rev [1]
	[IHFA_Cybersecurity]	[18/11/2025]
		Page 5 of 5

We constantly strive to maintain a high level of compliance, not only by adhering to current and mandatory regulations, but also by adopting international information security best practices. We understand that ensuring an effective and cutting-edge Information Security Management System (ISMS) requires investing in the right resources. Therefore, we confidently allocate adequate human, technological, and financial resources to implement, maintain, and continuously improve our ISMS.

Furthermore, we believe it is essential to define clear roles and responsibilities within our organization. This ensures effective and coordinated information security management, allowing us to minimize risks and best protect the sensitive data we are responsible for.

At Iacobucci HF Aerospace SpA, together with our senior management, we are committed daily to maintaining our Information Security Management System (ISMS) active, effective, and perfectly aligned with our corporate objectives. We understand the importance of staying abreast of regulatory and technological developments, which is why we adopt a dynamic and proactive approach.

We base our information security on simple principles which include, but are not limited to:

- information accessible only to those who need it (need to know principle);
- staff training courses on safety issues;
- controlled supply chain;
- principle of security by default by design.

To ensure continuous improvement, we set clear and measurable goals, ensuring they are specific, realistic, and achievable, as well as well-contextualized over time. This allows us to consistently maintain high information security quality and accurately monitor our progress.

We firmly believe in the value of data-driven decisions. We regularly conduct monitoring, measurement, and internal audits to gather reliable information and support sound and informed decision-making.

Furthermore, we constantly promote innovation and are open to the adoption of emerging technologies. We believe that this forward-looking mindset allows us to improve the efficiency and effectiveness of our ISMS, while maintaining high safety standards and quickly adapting to changes in the technological and regulatory environment.

Senior Management ensures that this policy is communicated clearly and transparently to all staff, using appropriate channels such as meetings, the company intranet, newsletters, and dedicated training activities. Furthermore, it is committed to promoting a culture of information security through training, awareness programs, and the active involvement of employees at all levels.

Ferentino, 09/12/2025

“Approved by the Board of Directors on 09/12/2025”