
	[Information Security Policy] Public	Section 1
		Rev [1]
	[IHFA_Cybersecurity]	[01/06/2023]
		p.1of19

[IHFA_Cybersecurity]

[Public]

[Information Security Policy]

	[Information Security Policy] Public	Section 1
	[IHFA_Cybersecurity]	Rev [1]
		[01/06/2023]
		p.2Of19


Revisions

Rev	Date	Causal	Editorial board	Verify	Approval
1	01/06/2023	First issue	Gyala	Iacobucci	Iacobucci

Pages modification

PAGE	REV.	DATE

ALL.	REV.	DATE

	[Information Security Policy]	Section 1
	Public	Rev [1]
	[IHFA_Cybersecurity]	[01/06/2023]
		p.30f19

SUMMARY

1. DECLARATION OF PRINCIPLES 5

2. General 6

2.1 Need for an Information Security Policy 6

3. Commitments 7

3.1 Brooms..... 8

3.2 Review, control and change management..... 8

3.3 Normative requirements 9

4. SECURITY ORGANIZATION AND RESPONSIBILITY 10

 Objective..... 10

 Direction..... 10

4.1 Steering Committee for Security (CDS) 10

4.2 Department Managers 10

4.3 Information systems manager 11

4.4 Responsible for the information security management system 12

4.5 Employees and collaborators 12

5. INFORMATION FLOWS WITH OTHER ORGANIZATIONS 13

6. RISK MANAGEMENT 14

6.1 Objective and methodology 14

7. OPERATIONAL CONTINUITY (BUSINESS CONTINUITY) 15

7.1 Objective 15

7.2 Requirements for operation 15

7.3 Planning elements 15

8. PHYSICAL AND ENVIRONMENTAL SAFETY 16

8.1 Objective 16


8.2 Area security 16

8.3 Premises security 16

8.4 Access control to premises 16

9. LOGICAL ACCESS CONTROL..... 17


9.1 Objective 17

	[Information Security Policy] Public	Section 1
		Rev [1]
	[IHFA_Cybersecurity]	[01/06/2023]
		p.40f19

9.2 Access to systems and applications..... 17

10. SECURITY OF NETWORKS AND COMMUNICATIONS 18

11. INCIDENT MANAGEMENT 19

	[Information Security Policy]	Section 1
	Public	Rev [1]
	[IHFA_Cybersecurity]	[01/06/2023]
		p.5Of19

1. STATEMENT OF PRINCIPLE


The Information Security Policy in Iacobucci HF Aerospace SpA aims to protect information assets from threats, whether they are organisational, technological, internal or external, accidental or intentional.

To this end, Iacobucci HF Aerospace SpA approves this document aimed at:

- ensure the confidentiality of information;
- maintain the integrity of information;
- ensure the availability of IT services;
- comply with regulatory and legislative requirements and internal rules;
- train staff on information security;
- track and analyze any incidents, real or suspected, affecting information security;
- establish rules, develop plans and adopt measures to implement an increasingly effective information security policy;

and also the purpose is also to:

- indicate the Management as responsible for the implementation of this Policy;
- establish that the Heads of Organizational Positions are responsible for the application and compliance with the Information Security Policy;
- assign each employee and/or collaborator responsibility for compliance with the Information Security Policy.

	[Information Security Policy] Public	Section 1
		Rev [1]
	[IHFA_Cybersecurity]	[01/06/2023]
		p.6Of19

2. GENERAL ASPECTS

The Iacobucci HF Aerospace SpA Information Security Policy is implemented to protect, at an optimal level and at a cost compatible with our specificities, the Information Management System, from events intended as threats or accidents, external and/or internal, objective and/or subjective, which can compromise the confidentiality, integrity and availability of information during all company processes.

The purpose of this document is to indicate the needs, objectives, purposes, and organizational models of the security strategy that Iacobucci HF Aerospace SpA intends to pursue, in order to guide its development, management and control.


2.1 NEED FOR AN INFORMATION SECURITY POLICY

The Company Information Assets represent the main resource for correctly managing customer relations, for planning the continuous innovation of the offer and guaranteeing the quality of the service of Iacobucci HF Aerospace SpA to its customers; as such, it must be adequately protected with a constant balance between the level of risk accepted and the corresponding degree of protection required, correctly combining the need to protect the value of information with the need to ensure the efficiency, effectiveness and the continuity of business processes.

Information is increasingly managed in electronic form and the systems are used by a growing number of stakeholders: this, if on the one hand allows their better accessibility and availability, on the other it determines profound and rapid changes in the risk scenarios that require presence of suitable measures and tools to secure information, guaranteeing its protection also in response to a growing demand for security from customers.

In such a context, Iacobucci HF Aerospace SpA governs the Security of the corporate Information assets in compliance with and on the basis of recognized standards, consolidated methodologies, contractual obligations, Laws and Regulations, binding requests deriving from third-party audits and due diligence operations.

However, information security is a managerial responsibility, not just a technological factor. With this conviction accompanied by the constant need to search for new market strategies aimed at giving guarantees, not only on the quality of the services provided, but also on the methods of processing information regarding customers, suppliers and other interested parties, as well as of its own structure organizational structure, Iacobucci HF Aerospace SpA has decided to implement an Information Security Management System modeled on the basis of the UNI CEI ISO/IEC 27001:2017 standard.

	[Information Security Policy]	Section 1
	Public	Rev [1]
	[IHFA_Cybersecurity]	[01/06/2023]
		p.70f19

3. ENGAGEMENTS


Given all of the above, Iacobucci HF Aerospace SpA, in compliance with the mandatory requirements and in particular with the legislation in force regarding the security of information and related information systems, undertakes to ensure that:

- The information is protected from unauthorized access, also by using encryption of data and communications, in compliance with confidentiality and is available to authorized users when they need it, this being a key aspect of the ISMS perimeter;
- The information is appropriately classified, since the classification of information constitutes the basic activity for the assessment of risk and therefore of the potential damage to corporate data and information;
- The information is not disclosed to unauthorized persons as a result of deliberate or negligent actions and, in respect of integrity, is safeguarded from unauthorized modifications;
- Business continuity plans are drawn up and that these plans are kept up-to-date and controlled as far as possible;
- Personnel receive training and updates on information security;
- Suppliers of technologies and services related to the provision/management of systems and services, in particular as regards the purchase of IT components for data centers and for customers, are carefully selected and monitored with the same criteria and principles that Iacobucci HF Aerospace SpA adopts for its internal processes;
- All information security breaches and possible weaknesses are reported to the ISMS Manager and investigated;
- The contractual requirements are respected;
- In implementing the above, there is always a commitment to continuous improvement along the entire value chain, both in the management of information and data and in the supporting technological and documentary infrastructure.

Through the implementation of this policy, Iacobucci HF Aerospace SpA intends to comply with the commitment to comply with the UNI CEI ISO/IEC 27001:2017 standard as well as achieve and maintain this certification.

To achieve this objective, the Management of Iacobucci HF Aerospace SpA undertakes to ensure that this policy is disseminated, understood and implemented not only by internal personnel, but also by interns, external collaborators, consultants, suppliers, with particular attention to outsourcers who are in any way involved with corporate information security.

Lastly, the Management of Iacobucci HF Aerospace SpA undertakes to regularly review this Policy and any changes that may affect it, to ensure that it remains suitable for the business and the company's ability to satisfy Customers, Suppliers and other interested parties.

	[Information Security Policy] Public	Section 1
		Rev [1]
	[IHFA_Cybersecurity]	[01/06/2023]
		p.8Of19

3.1 SCOPE

Iacobucci HF Aerospace SpA considers the management system and the information managed, due to the particular importance they assume for the pursuit of its corporate purposes, an integral part of its assets. It is an objective of absolute priority for Iacobucci HF Aerospace SpA to safeguard the security of its information system and to protect the confidentiality, integrity and availability of the information produced, collected or in any case processed, from any intentional or accidental, internal or external threat.


In this context it means:

- Confidentiality** the guarantee that specific information is protected from improper access and is used exclusively by authorized parties.
- Integrity** the guarantee that all information is actually the one originally entered in the computer system and has been legitimately modified by authorized parties.
- Availability** the guarantee of availability of information in relation to the need for continuity of service delivery and compliance with the rules that require its safe conservation.
- Authenticity** the guarantee that the information received corresponds to that generated by the person or entity that transmitted it.

Iacobucci HF Aerospace SpA bases its information protection policy on an appropriate Risk Analysis of all the resources (assets) that make up the information management system, in order to understand vulnerabilities, assess possible threats and prepare the necessary countermeasures.

3.2 REVIEW, CONTROL AND CHANGE MANAGEMENT

The Iacobucci HF Aerospace SpA Management is responsible for the periodic review of the Policy so that it is aligned with any significant changes that have occurred in the organization and/or in the technologies used to protect information. In the event of significant changes, these will be managed, with specific projects, documented by a defined Manager, according to the area of competence.

	[Information Security Policy]	Section 1
	Public	Rev [1]
	[IHFA_Cybersecurity]	[01/06/2023]
		p.90f19

3.3 NORMATIVE REQUIREMENTS

The matter of information security is governed by Community legislation and by Italian legislation. Here are the most recent and most important standards on the protection of personal rights and the standards that specifically refer to the ISO 27001 system.

Legislation on the protection of personal rights

Legislative Decree 10 August 2018, n. 101 Provisions for the adaptation of national legislation to the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data, as well as on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation). (GU n.205 of 4-9-2018) In force on: 19-9-2018.

Law n. 163 of 10/25/2017 in particular article 13 Delegation to the Government for the transposition of European directives and the implementation of other acts of the European Union - European Delegation Law 2016-2017.

Regulation 2016/679 of the European Parliament and of the Council, of 04/27/2016 concerning the protection of individuals with regard to the processing of personal data, as well as the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) published in the OJEU of 4 May 2016, entered into force on 24 May 2016, applicable directly in all EU countries from 25 May 2018.

Legislative decree n. 196 of 06/30/2003 Code regarding the protection of personal data.


Legislation referring to the ISO 27001 certification of paying agencies

Reg. (EC) 11/03/2014, n. 907/2014 "Commission Delegated Regulation supplementing Regulation (EU) No. 1306/2013 of the European Parliament and of the Council as regards paying agencies and other bodies, financial management, clearance of accounts, securities and the use of the euro".

ISO 27001 standard which defines the requirements for setting up and managing an Information Security Management System (ISMS or ISMS), and includes aspects relating to logical, physical and organizational security.

ISO 27002 guidelines which constitute a collection of "best practices" that can be adopted to meet the requirements of the ISO 27001:2017 standard in order to protect information assets.

ISO 27005 guidelines "Information technology - Security techniques - Information security risk management"; their purpose is to provide guidelines for information security risk management, defining rigorous methods for risk analysis and the related creation of a risk prevention/containment plan.

	[Information Security Policy]	Section 1
	Public	Rev [1]
	[IHFA_Cybersecurity]	[01/06/2023]
		p.10Of19

4. SECURITY ORGANIZATION AND RESPONSIBILITY

The organization and responsibility of security relates to the identification of the procedures aimed at managing and controlling the security measures adopted and takes the form of identifying the roles, functions and responsibilities involved in the creation and management of the Information Security System.

1.1.1 Objective

Ensure that managers and collaborators, considering that information security is a common responsibility, are adequately informed and trained on the role they can play in order to minimize the risks deriving from threats to the security of the information management system.

1.1.2 Direction

The Management is responsible for the contents of the Information Security Policy, for its issuing, implementation and updating. The Management makes use of the technical and organizational support of the Steering Committee for Security (CDS) for the definition and implementation of the Information Security Policy.

4.1 STEERING COMMITTEE FOR SECURITY (CDS)

The CDS (Directive Committee for Safety) is the decision-making body in terms of policies and investments to be supported and its composition, defined in harmony with the organization of Iacobucci HF Aerospace SpA, is described below in this paragraph.

Participation in the CDS can be expanded from time to time if there is a need to examine specific topics. The CDS has the function of supporting the Management in the research and indication of the guidelines and the best methods of application of the Information Security Policy.


The CDS is made up of:

- Management
- Responsible for the information security management system

The CDS meets annually, except for specific needs. In the absence of specific safety issues, the Management Review meeting has the value of an annual meeting.

4.2 DEPARTMENT MANAGERS

It is the responsibility of the function managers to ensure that:

	[Information Security Policy]	Section 1
	Public	Rev [1]
	[IHFA_Cybersecurity]	[01/06/2023]
		p.11Of19


- a) their collaborators
- are informed of the confidentiality clauses forming an integral part of the employment contract;
 - are educated, through special courses, provided for in the "Annual Training Plan", about their responsibility with respect to information security;
 - are authorized to access systems or applications or data following the defined authorization profiles, consistent with the role and activities performed. The communication for the authorization of access rights is carried out in compliance with the specific access procedures of the systems or applications or data;
 - are trained in the use of the computer systems for which they have been authorized;
 - have access to and have read the information security policies of Iacobucci HF Aerospace SpA;
- b) the documentation of the processes relating to information management activities is updated so that all the work activities deemed critical can be carried out continuously in the event of unavailability of the assigned collaborators;
- c) changes in the duties or activities of collaborators (for example in the case of organizational changes) which involve variations in the access profile to systems, applications and data, are communicated to the Information Security Manager, to vary or, if necessary, cancel the profile and login credentials. The communication must be made in compliance with the specific access procedures.

4.3 INFORMATION SYSTEMS MANAGER

He takes care of the development and evolutionary and corrective maintenance of the IT systems of Iacobucci HF Aerospace SpA. He is responsible for the activities envisaged by the back-up and logical access procedures and for the activities relating to business Continuity and the relevant Disaster recovery.

Collaborates in the management of incidents related to information security and in the management of changes to the technological infrastructure, assessing the risks and related impacts.

As System and Information Security Administrator, he carries out the management, in terms of security aspects, of the systems responsible for data processing managed on behalf of the Data Controller and according to the latter's indications.

	[Information Security Policy]	Section 1
	Public	Rev [1]
	[IHFA_Cybersecurity]	[01/06/2023]
		p.12Of19

4.4 RESPONSIBLE FOR THE INFORMATION SECURITY MANAGEMENT SYSTEM


The Information Security Management System Manager defines, in agreement with CDS, the Information Security Management System development plan in compliance with the objectives of Iacobucci HF Aerospace SpA.

The Manager also provides a suitable guarantee of full compliance with the provisions in force regarding information security and its processing. Organizes and supervises, in collaboration with the Management, the creation of the "security structure" aimed at preventing and protecting the company's information assets from threats and critical events in order to guarantee the continuity of the company's core business.

4.5 EMPLOYEES AND COLLABORATORS

Each employee or collaborator, in any capacity, is required:


- compliance with the information security measures and the application of the relative procedures in the performance of his/her work activities;
- to report violations of information security measures, adopting the procedure in force.

	[Information Security Policy] Public	Section 1
		Rev [1]
	[IHFA_Cybersecurity]	[01/06/2023]
		p.13Of19

5. INFORMATION FLOWS WITH OTHER ORGANIZATIONS

Exchanges of information with certain external structures, bodies and/or public and private organizations are managed without compromising the integrity and confidentiality of the information, guaranteeing the security and correctness of the functioning of the processing and communication systems.

The information flows with external subjects are characterized by compliance with the agreed rules in order to preserve the integrity, confidentiality, authenticity of the information exchanged and the security of the processing systems in compliance with the national and EU legislation in force.

	[Information Security Policy] Public	Section 1
		Rev [1]
	[IHFA_Cybersecurity]	[01/06/2023]
		p.14Of19

6. RISK MANAGEMENT

6.1 OBJECTIVE AND METHODOLOGY


The objective of the Risk Analysis is to identify and counter possible threats to the security of corporate systems and information, in order to prepare adequate prevention and protection measures.

Risk Analysis is the main element from which all control activities, security Policies and operating procedures related to information security derive.

In this regard, Iacobucci HF Aerospace SpA adopts its own methodology which allows it to:

- Analyze and rank the risks and opportunities in the organization (Analysis at the security process level: what is acceptable and what is not);
- Assess and plan actions to address risks (avoid, eliminate or mitigate risks);
- Implement the defined plan (Conduct actions);
- Check the effectiveness of the actions;
- Learning from experience (Continuous Improvement).

The Risk Analysis is conducted on a periodic and regular basis, to guarantee the continuing effectiveness of the mitigation measures identified and implemented.

	[Information Security Policy]	Section 1
	Public	Rev [1]
	[IHFA_Cybersecurity]	[01/06/2023]
		p.15Of19

7. OPERATIONAL CONTINUITY (BUSINESS CONTINUITY)

The responsibility for "Operational Continuity" lies with the Management which prepares the Business Continuity Plan - BCP, understood as an indication of the organizational and technological activities, aimed at the continuity of the processes that contribute to the mission of Iacobucci HF Aerospace SpA.

In preparing the aforementioned Plan, the Management makes use of the technical and organizational support of the Steering Committee for Safety (CDS).

7.1 OBJECTIVE

The objective of Business Continuity Management is to ensure the continuity of the organization's essential processes/services (critical processes) at a given level of service, in the event of a disastrous event.


7.2 REQUIREMENTS FOR OPERATION

Iacobucci HF Aerospace SpA through the precautions contained in the BCP believes it can contain the impact of any disastrous events, within the scope of the recovery requirements defined.

7.3 PLANNING ELEMENTS

The methodologies that allow you to draw up, create and maintain a BCP are different and refer to standards issued by important international institutes. The common elements are:

- identification of the coordination structures of the recovery strategy;
- evaluation of the results of the Business Impact Analysis for the identification of critical processes and services and intervention priorities;
- preparation of the procedures to be carried out in the event of implementation of the BCP;
- development, documentation and verification of the BCP.

	[Information Security Policy] Public	Section 1
		Rev [1]
	[IHFA_Cybersecurity]	[01/06/2023]
		p.16Of19

8. PHYSICAL AND ENVIRONMENTAL SAFETY

It constitutes the form of protection that pertains to the protection of information processing systems and manifests itself with physical measures aimed at guaranteeing the control services against unauthorized access to the premises where the information management systems are located, in order to preserve the integrity and availability of Iacobucci HF Aerospace SpA's information processing systems.

8.1 OBJECTIVE

Minimize the impacts of threats to information processing systems due to damage or intrusion.

8.2 AREA SECURITY


The areas that include the premises where the information management systems of Iacobucci HF Aerospace SpA reside are equipped with controlled access doors.

8.3 PREMISES SECURITY

The premises are equipped with systems designed to guarantee and maintain the safety and integrity of the equipment and systems, in order to avoid failures that can cause physical interruption to the functioning of the activities.

8.4 ACCESS CONTROL TO PREMISES

All systems and network equipment are located in secure buildings with controlled access. In particular, the area where the server systems of the information system reside at the CED is identified as a "restricted access area" and admission is permitted only in the presence of authorized internal personnel, as required by internal procedures.

	[Information Security Policy] Public	Section 1
		Rev [1]
	[IHFA_Cybersecurity]	[01/06/2023]
		p.17Of19

9. LOGICAL ACCESS CONTROL

9.1 OBJECTIVE

Prevent unauthorized access through control procedures, protect information and processing and communication systems with technological and organizational measures designed to guarantee access control, the quality of information, as well as their confidentiality and integrity.

9.2 ACCESS TO SYSTEMS AND APPLICATIONS


Access to applications (permissions)

Iacobucci HF Aerospace SpA defines the authorizations and access policies in relation to the role in the company and the pertinent activities.

Iacobucci HF Aerospace SpA adopts user profiling, both internal and external, for granting access credentials to applications and uses a "formal procedure" for this purpose, maintaining documentation of the authorizations granted.

The Information Security Manager periodically checks, at least once a year, the functional validity of all active authorizations for access to Iacobucci HF Aerospace SpA applications.


The revocation of access to the information processing systems of Iacobucci HF Aerospace SpA is implemented when the enabling characteristics of a user lapse.

	[Information Security Policy] Public	Section 1
		Rev [1]
	[IHFA_Cybersecurity]	[01/06/2023]
		p.18Of19

10. SECURITY OF NETWORKS AND COMMUNICATIONS

To ensure the security of networks and communications, it is necessary to prevent access to networks and the illegal use of information by unauthorized parties in order to preserve data confidentiality and service availability.

The "Internal Disciplinary" contains the recommendations on the security of the internal network, the rules for browsing the Internet and the indications for the appropriate use of e-mail and protection against malicious software.

	[Information Security Policy] Public	Section 1
		Rev [1]
	[IHFA_Cybersecurity]	[01/06/2023]
		p.19Of19

11. INCIDENT MANAGEMENT

An incident in the field of information security is a suspicious event or a vulnerability such as to violate the integrity, confidentiality and/or availability of applications, data and/or information processing systems.

All users must comply with the instructions received on information security and contained in the "Internal regulations" and in the information security incident management procedure.

Tullio De Santis

IT, Security and Information Compliance Officer