CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

This document is provided for information purposes only and constitutes a courtesy English translation of the original Italian-language version.

In the event of any discrepancy, inconsistency or conflict, the Italian-language version shall prevail and shall be the only legally binding version.

CYBER 4.0

ORGANIZATION, MANAGEMENT AND CONTROL MODEL PURSUANT TO LEGISLATIVE DECREE 231/2001 GENERAL SECTION

GENERAL SECTION

Version	Data	ApprovaL
01	28/02/2024	CMC
02	22/01/2026	CMC

SUMMARY

Abbreviations and definitions

Cyber or the Association or, alternatively, Competence Centre	Cyber 4.0., National highly specialized Competence Centre for cybersecurity.
Legislative Decree no. 231/2001 or Decree	Legislative Decree no. 231 of 8 June 2001, concerning "Regulation of the administrative liability of legal persons, companies and associations, including those without legal personality, pursuant to Article 11 of Law no. 300 of 29 September 2000" (in Gazzetta Ufficiale no. 140 of 19 June 2001), subsequent amendments and integrations
Model	Organization, management and control model provided for and regulated by Articles 6 and 7 of Legislative Decree no. 231/2001.
NCBAs	National Collective Bargaining Agreements applied by the Association to its employees.
Recipients	Subjects obliged to comply with the Model, as well as all the annexes that form an integral part thereof, specifically: - the members of the Assembly, - the members of the Coordination and Management Committee (CMC); - the members of the Scientific and Steering Committee (SSC); - the members of the Control Body; - the members of the Supervisory Body; - the President and the Vice-President of the Association; - Personell; - the Collaborators and Consultants; - Commercial Partners; - the Clients and/or the companies served; - the Suppliers of goods and services, continuous or occasional;

	- anyone who, for any reason or activity, operates in the interest, name, and on behalf of the Association or maintains relationships of any nature with it.
Code of Ethics	The Association's Code of Ethics and its subsequent updates: general principles and behavioral rules that Cyber is inspired by in conducting its social activities, containing the set of rights, duties, and responsibilities of the entity towards its stakeholders
Control Body o CB	Body established by the entity and endowed with autonomous powers of initiative and control, responsible for supervising the functioning and observance of the Model, as well as its relevant updating
Predicate Offences Reati presupposto	The offences covered by Legislative Decree No. 231/2001, as subsequently amended and supplemented.
Disciplinary System or Sanctioning System	A suitable system for sanctioning the failure to comply with the principles, prescriptions, and standards of behavior indicated in the Code of Ethics and the Model, including the Procedure for managing reports
Legislative Decree no. 24/2023 or Whistleblowing Decree	Legislative Decree no. 24 of 10 March 2023, concerning: "Implementation of Directive (EU) 2019/1937 of the European Parliament and of the Council, of 23 October 2019, regarding the protection of persons who report breaches of Union law and containing provisions concerning the protection of persons who report breaches of national legal provisions"
Manager	Pursuant to Article 4, paragraph 2 of Legislative Decree no. 24/2023, "an autonomous internal person or office dedicated and with specifically trained personnel for managing the reporting channel" or "the external entity, also autonomous and with specifically trained personnel"

1. CYBER 4.0.

Cyber 4.0, was established on April 10 2019, and represents a public-private partnership involving various actors of national importance as members, including representatives of universities, research bodies, public institutions, large companies, foundations, and highly specialized SMEs. The Association is one of the 8 national highly specialized Competence Centres, established and co-financed by the Ministry of Enterprises and Made in Italy, and it is the only one entirely focused on **cybersecurity**. Its establishment aligns with the Ministerial Decree D.D. 29.01.2018 of the Directorate General for Industrial Policy, Competitiveness and Small and Medium Enterprises (DGPICPMI), implementing the Decree of the Ministry of Economic Development in concert with the Ministry of Economy and Finance no. 214 of 12.09.2017.

Launched within the context of the Industry 4.0 plan, the Centre is currently recognized as a national technology transfer hub. It also serves as the implementing entity of the **PNRR** (National Recovery and Resilience Plan) on behalf of the MIMIT (Ministry of Enterprises and Made in Italy) (Mission 4, Component 2, Investment 3). This role includes acting both as a National Competence Centre and as the coordinator/leader of the EDIH – European Digital Innovation Hub project named **NEST** (Network for European Security and Trust), which received the Seal of Excellence from the European Commission. Furthermore, the Centre is a partner of two Houses of Emerging Technologies (Cagliari Digital Lab and Pesaro CTE SQUARE).

In addition to its institutional activities, Cyber provides operational services related not only to cybersecurity but also to all so-called Emerging Technologies, in response to specific market requests, through one or more members. The Association aims to develop, coordinate, and implement a program of activities, also through participation in national and European public tenders. This program includes orientation and training services for businesses, as well as the implementation of innovation, industrial research, and experimental development projects. These activities are designed to enable beneficiary businesses, especially SMEs, to create new products, processes, or services or improve existing ones, with a particular focus on the automotive, healthcare, and aerospace sectors.

The mission is to accompany policy makers, businesses, and Public Administrations or Public Entities on a growth path toward secure digitalization. This is achieved through concrete, strategic, and sustainable solutions based on knowledge, innovative technologies, and enabling services developed with the expertise of its network, thereby enhancing the country's excellence in the European and international context.

1.1 The organizational structure

The governance Model of Cyber 4.0, and the overall organizational system, are structured to ensure the implementation of strategies and the achievement of statutory objectives.

The Association has adopted the following governance system

The bodies of the Association are:

- Assembly;
- the President and the Vice President of the Association;
- the Coordination and Management Committee;
- Scientific and Steering Committee;
- Control Body

The **President** is the legal representative of the Association and is responsible for convening and chairing the Assembly and the Coordination and Management Committee.

The **Coordination and Management Committee** (CMC) is composed of between 5 and 15 members (representing the Shareholders) and is the body vested with powers for the ordinary and extraordinary management of the Association.

The **Scientific and Steering Committee** (SSC) has a consultative role and is composed of representatives of members and highly qualified external experts in cybersecurity/emerging technologies.

The **Control Body** periodically verifies the formal and substantive regularity of the accounting and certifies the regularity of the budget and final accounts.

The **execution structure** is coordinated by a Chief Operating Officer, who oversees five functions: Administration and Finance, Research and Innovation, Training and Advisory, Business Development, and Communication. These functions operate cross-sectorally across the four reference sectors: Core Cybersecurity, Automotive, Space, and E-health

2. The Organization, Management and Control Model

2.1 The adoption and updating of the Model

Association decided to adopt a Model consistent with the requirements of Legislative Decree no. 231/2001, viewing it as part of a continuous improvement process aimed at guaranteeing correctness and transparency in pursuing its associative objectives. Cyber believes that adopting the Model is a valuable tool, beyond legal requirements, for raising awareness among the Administrative Body, statutory bodies, employees, collaborators, and all Recipients, ensuring business activities comply with legal obligations and industry best practices.

Cyber 4.0 has also obtained certifications according to the standards UNI ISO 9001:2015 (Quality management systems - Requirements) and UNI ISO 27001:2022 (Information security, cybersecurity and

privacy protection - Information security controls). The Association's Control and Management Committee approved the first version of the Model, along with the Code of Ethics, with a resolution dated 28.02.2024, and subsequently appointed the Supervisory Body. In preparing the Model, the Association considered the discipline under Legislative Decree no. 231/2001, as well as the principles expressed by Confindustria in the Guidelines approved by the Ministry of Justice.

Regarding the whistleblowing reporting management system (Section 6 of the Model), the Association considered the provisions of the Whistleblowing Decree (D. Lgs. n. 24/2023), the Guidelines approved by ANAC with resolution no. 311 of July 12, 2023, and the Operational Guide approved by Confindustria in October 2023. The Model must be periodically revised and re-examined to ensure its updating and adequacy. The exclusive responsibility for formulating any modifications and integrations to the Model rests with the Coordination and Management Committee (CMC), even when based on notifications from the Control Body

For example, updating the Model becomes necessary in the event of:

a) legislative changes concerning the administrative liability of entities for offenses dependent on crime;
b) significant changes to the Association's organizational structure or sectors of activity
c) or significant violations of the Model and/or a negative outcome in the effectiveness checks conducted by the Control Body.

2.2 The creation of the Model

The Model complements the internal regulatory system and the management systems implemented by the Association, aiming for integrated risk management concerning non-compliance. It incorporates common procedures designed for efficiency and streamlining, avoiding overlapping roles or duplicated checks and corrective actions in processes where roles intersect

The creation process involved several steps::

- identifying sensitive processes: This phase involved analyzing the business context to identify the area/sector of activity and the potential methods by which crimes could occur, resulting in a representation of sensitive processes, risk areas, existing controls, and potential critical issues;
- conducting the gap analysis: Based on the existing situation, necessary initiatives were identified to best align the internal control system and essential organizational requirements with the objectives of the Decree
- Defining the decision-making procedures

- Carrying out a historical analysis ("case history") of any past cases involving criminal, civil, or administrative precedents against the Association or its employees relevant to the legislation introduced by Legislative Decree no. 231/2001
- Defining the Model;
- Establishing a Control Body tasked with overseeing the Model's functioning and observance, and proposing and managing its updating
- Appointing the Whistleblowing Report Manager, in compliance with Legislative Decree no. 24/2023, the ANAC Guidelines (resolution no. 311 of July 12, 2023), and the Confindustria Operational Guide (October 2023).

Fundamental elements of the Model include:

- Mapping the Association's "sensitive activities," meaning the activities where crimes may be committed;
- Attributing to the Supervisory Body suitable powers to supervise the effective and correct functioning of the Model, and to manage its updating and refinement, including potentially utilizing external parties
- Verifying and archiving documentation for every relevant operation under Legislative Decree no. 231/2001, allowing for ex-post verification of monitored operations
- Respecting the principle of separation of duties in high-risk areas
- Defining authorization powers consistent with assigned responsibilities
- Integrating the Model with existing procedures and operating instructions aimed at overseeing areas of activity and preventing the commission of crimes provided for by the Decree;
- Carrying out awareness-raising and dissemination activities, including training and information at all company levels regarding established behavioral rules and procedures.

2.3 Purpose of theh Model

The **purposes** of the Model are

- To prevent and reasonably limit possible risks connected to the company activity, focusing particularly on eliminating or reducing any illegal conduct.
- To create awareness among all those who operate in the name and on behalf of the Association in risk areas that violations of the Model's provisions may result in criminal and administrative sanctions not only against them but also against the Association.

- To disseminate the company culture that the Association does not tolerate unlawful behavior, regardless of type or purpose, as such behavior violates current laws and is contrary to the general principles and behavioral rules specified in the Code of Ethics

2.4 Recipients of the Model

The Recipients are obligated to strictly comply with all provisions of the Model, including the annexes and the Reporting Management Procedure, in fulfillment of their duties of loyalty, fairness, and diligence arising from the employment relationships established with the Association.

2.5 The structure of the Cyber 4.0 Organization, Management and Control Model

The Model consists of

- "**General section":** this includes annexes (listed at the bottom of the Model) and contains a description of the preparatory work and criteria used in drafting the Model, its structure, its main elements (such as the Supervisory Body, the whistleblowing system, and the disciplinary system), and the objectives pursued through its adoption;
- "**Special Section":** this includes integral annexes and identifies the processes within which the crimes referred to in Legislative Decree no. 231/2001 may be committed, along with the relevant protocols (or specific control Standards) for the identified sensitive activities;
- "**Code of Ethics":** A document that sets the guidelines, general principles, and behavioral rules that guide the Association in conducting its activities

The "**Procedure for reporting management**": Considered an integral and substantial part of the Model, this document establishes the rules for managing whistleblowing reports in accordance with Legislative Decree 24/202.

3. The Supervasory body

Article 6, paragraph 1, letter b) of Legislative Decree no. 231/2001 mandates, as an essential prerequisite for exemption from liability following the commission of crimes, the establishment of an internal body endowed with autonomous powers of initiative and control. This body is tasked with supervising the Model's functioning and observance and managing its updating

The Supervasory Body (SB) must be promptly informed, via a specific and dedicated communication channel, about any acts, behaviors, or events that could lead to a violation of the Model or are otherwise relevant for

the purposes of Legislative Decree no. 231/2001. All information and communications must be provided in writing using the e-mail address: **odv@cyber40.it**. The general principles regarding the SB's institution, appointment, replacement, functions, powers, specific reporting obligations to it, and its reporting activity to the Control Bodies are defined in **Annex no. 2** ("Supervasory Body").

4. The Whistleblowing system

To ensure responsible management aligned with legal requirements and to encourage Recipients to report unlawful phenomena, Cyber 4.0 has adopted a *whistleblowing* reporting management system.

This system complies with the following regulations:

- Legislative Decree No. 24/2023 (Whistleblowing Decree), implementing Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019, on the protection of persons who report breaches of Union law, and laying down provisions on the protection of persons who report breaches of national statutory provisions.
- Guidelines approved by talian National Anti-Corruption Authority (ANAC) with resolution no. 311 of July 12, 2023;
- The Operational Guide approved by Confindustria in October 2023;
- UE regulation 2016/679, c.d. GDPR.

Specifically, Cyber 4.0, after consulting the trade union representatives referred to in Article 51 of Legislative Decree no. 81/2015, as required by Article 4, paragraph 1, of the Whistleblowing Decree, has established an internal reporting channel (the so-called whistleblowing channel) that allows reports to be submitted, both in written and oral form, using the system of guarantees and protections provided for by the Whistleblowing Decree.

This channel consists of a platform (Legality Whistleblowing by DigitalPA) that complies with the requirements set out in the Whistleblowing Decree. The platform can be accessed at https://cyber40.segnalazioni.net and is published on the Association's institutional website in the "Ethics and Compliance" section (https://www.cyber40.it/etica-e-compliance/).

The entire operation of the whistleblowing channel is explained in the "Procedure for the Management of Reports" (hereinafter, the "Procedure") adopted by the Association, which forms an integral part of the 231 Model, to the contents of which full reference is made.

The Procedure is published on the Association's institutional website within the dedicated section (https://cyber40.segnalazioni.net/contenuti/files/Cyber40_Procedura_gestione_segnalazioni_whistle_def22.pdf).

The entity entrusted with the management of the whistleblowing channel (the so-called "Manager") must meet the following requirements:

- autonomy (impartiality and independence);
- specific training.

The management of whistleblowing reports is entrusted to the Supervisory Body, which operates with full autonomy, impartiality, and independence and has received appropriate and specific training. The relevant duties and responsibilities are assigned to it through the execution of a specific agreement, which also governs aspects relating to the processing of personal data, in accordance with the provisions of the Whistleblowing Decree and as further specified in the Procedure, to which full reference is made.

The Supervisory Body is the o**nly function authorized** to access the secure area of the whistleblowing platform and to receive, assess, and manage reports. No oversight, direction, or interference in the handling of reports may be exercised by the Administrative Body or by any other governing or management body of the Association.

The Administrative Body is responsible only for **monitoring the effective and proper functioning** of the whistleblowing system and the related Procedure.

The whistleblowing system does not apply to complaints, claims, or requests relating exclusively to the personal interests of the reporting person that concern their individual employment relationship or relations with line management.

Cyber 4.0, as also expressly stated in the Procedure, prohibits any act of retaliation carried out as a result of a whistleblowing report, as well as any act intended to hinder (or attempt to hinder) the submission of a report, and sanctions any violation of the Whistleblowing Decree (including retaliation, obstruction of reporting, breaches of confidentiality obligations, failure to follow up on reports, etc.), as further illustrated in paragraph 5 of this General Part of the 231 Model and in the related Annex 3, as well as in the Procedure.

5. The sanctioning system

This system is designed to sanction any non-compliance with the principles, provisions and standards of conduct laid down in the Code of Ethics, the Model and the internal regulatory framework, ensuring their due observance. Any violation of the obligations defined in the Model, even if allegedly justified by the pursuit of a corporate interest, shall constitute a contractual breach or a disciplinary violation.

The sanctioning system, defined in **Annex 3** of the Model ("The sanctioning system"), outlines the specific sanctions and methods in case of violation or non-observance of obligations, duties, and/or procedures set in the Model.

If it is proven that a Recipient has committed a crime, the Association reserves the right to seek compensation for any damage caused.

6. Training and information

Cyber 4.0 To ensure the effective implementation of the Model, Cyber 4.0 deems it essential and takes steps to guarantee the correct and appropriate communication of its contents and principles throughout and beyond the organization.

The competent Function manages personnel training in close cooperation with the Supervisory Body. The SB must report to the Administrative Body any detected deficiencies in the training of the Association's personnel during the performance of its duties.

The training program must meet the following requirements:

- It must be adequate based on the position held by the recipients within the organization (new hire, employee, executive body member, statutory body member, etc.).
- The content must be different according to the activity performed by the subject (executive activity, high-risk activity, control activity, non-risk activity, etc.).
- The speaker must be a competent, authoritative person possessing the necessary professional qualifications to ensure the quality and suitability of the content discussed.

Participation in the training programme shall be mandatory, and specific monitoring mechanisms shall be defined in order to verify both attendance by training recipients and the level of knowledge and understanding achieved by each participant. Cyber 4.0 also ensures training for all personnel, including those who may be involved, in any capacity, in the management of whistleblowing reports, on the applicable whistleblowing framework and on the functioning of the internal reporting channel.

In particular, the training programme shall cover, at a minimum: the relevant regulatory framework on whistleblowing and personal data protection; the duties and responsibilities of the Whistleblowing Function and the procedures for submitting reports in cases where the latter may be affected by a conflict of interest; the general principles of conduct applicable to all recipients of the 231 Model and of the Procedure for the Management of Reports.

Participation in whistleblowing training courses is mandatory for employees and for all individuals who collaborate with or otherwise perform work activities for the Association. Non- participation in such training is subject to disciplinary measures, as provided for in paragraph 5 and Annex 3 of this General Part of the 231 Model, as well as in the Procedure for the Management of Reports, to which full reference is made. Documentation relating to training activities shall be retained by the Association and made available for consultation by the Supervisory Body and by any other duly authorized party.

6.1 Training and information for personnel

Training and information for internal personnel must take place through the following activities:

- Publication of the Model in the company repository, with non-segregated access for consultation by all employees.
- An initial training session.
- Periodic update meetings (including e-learning) and/or update e-mails (in case of changes to the company structure, modifications/revisions of internal operating procedures, or regulatory updates affecting the area covered by the Model).

Adequate information is also ensured in the event of updates or material changes to the 231 Model and to the “Procedure for the Management of Reports”.

Internal personnel are thus required to:

- acquire awareness regarding the Model's principles and contents,
- understand the operational methods for performing their activities,
- actively contribute to the Model's effective implementation, including reporting any deficiencies found.

6.2 Information for external Collaborators

The Association promotes awareness and understanding of the principles and standards of conduct set out in the Code of Ethics and the Model. To this end, Cyber 4.0 makes the Code of Ethics and the Model easily accessible to consultants, external collaborators, customers, suppliers, business partners, and any other parties engaged in commercial and/or professional relationships with the Association by sharing the relevant contents on the Association's website.

Accordingly, these parties will be provided with clear information, and procedures will be established to include and obtain their acceptance of specific contractual clauses, which will be integrated into the relevant standard contract templates.

Likewise, Cyber 4.0 ensures adequate and clear information on the whistleblowing channel (including the support measures offered by third-sector entities), both on its institutional website and at the workplace, for the benefit of members, suppliers, collaborators, business partners, and all other recipients of the Model, in accordance with the methods described in the "Procedure for the Management of Reports," to which full reference is made.

Appropriate and timely information is also ensured in the event of updates or material amendments to the 231 Model and to the "Procedure for the Management of Reports.

7. Anexes to the General Section of the Cyber 4.0 Organizational Model

Ann. 1) List of crimes provided for by Legislative Decree no. 231/2001 and subsequent amendments;

Ann. 2) Supervisory Body;

Ann. 3) Sanctioning System.