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.**

# ASSOCIATION CYBER 4.0

# CODE OF ETHICS

## 22/01/2026

**SUMMARY**

## 1. Introduction

Cyber 4.0, established on April 10, 2019, is the result of a public-private partnership involving several nationally relevant actors as members, including representatives from universities and research institutions, public institutions, large enterprises, foundations, and highly specialized SMEs.

The Association is one of the eight national high-specialization Competence Centers, established and co-financed by the Ministry of Enterprises and Made in Italy, and is the only one entirely focused on cybersecurity. It was created in line with the provisions of the 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 agreement with the Ministry of Economy and Finance n. 214 of 12.09.2017.

Launched in the context of the Industry 4.0 plan, the Center is now recognized as a national technology transfer hub and acts as an implementing body of the PNRR on behalf of MIMIT (Mission 4, Component 2, Investment 3), both as a National Competence Center and as coordinator/lead of the EDIH – European Digital Innovation Hub project called NEST (Network for European Security and Trust), which received the Seal of Excellence from the European Commission.

The Center is also a partner of two Emerging Technology Hubs (Cagliari Digital Lab and Pesaro CTE SQUARE).

Alongside its institutional activities, Cyber 4.0 provides operational services not only in cybersecurity but also in all so-called Emerging Technologies, in response to specific market requests, through one or more members.

Through participation in national and European public calls, the Association aims to develop, coordinate, and implement a program of activities – including guidance and training services for companies as well as the implementation of innovation, industrial research, and experimental development projects – aimed at enabling beneficiary companies, particularly SMEs, to create new products, processes, or services or to improve existing products, processes, or services, with a particular focus on the automotive, healthcare, and aerospace sectors.

Its mission is to support policymakers, enterprises, and Public Administrations or Public Bodies on a path of growth towards secure digitalization, through concrete, strategic, and sustainable solutions based on knowledge, innovative technologies, and enabling services developed with the expertise of its network, highlighting the country's excellence in the European and international context.

## 2. Code of Ethics

The Code of Ethics is an essential component of the Organization, Management, and Control Model adopted by the Association in compliance with Legislative Decree no. 231/01 and subsequent amendments and additions (hereinafter also referred to as the "231 Model") and conforms, in terms of content, to the guidelines contained in the Confindustria Guidelines and the ANAC Guidelines.

Through the Code of Ethics, Cyber 4.0 specifically aims to:

- Declare the ethical values and principles that guide its activities and its relationships with clients, suppliers, members, employees, and all other parties involved – in any capacity – with the Association;
- Express its commitment to conduct itself according to principles of fairness and equality, protection of the individual, diligence, transparency, confidentiality, impartiality, and the safeguarding of health and the environment;
- Summarize the fundamental principles, directives, and behavioral requirements that all those who, directly or indirectly, permanently or temporarily, establish any form of collaboration or act in the interest of the Association must apply in the conduct of business and the management of corporate activities.

**2.1 Recipients**

This document is binding for all those who participate in the sphere of interests of Cyber 4.0 for reasons of work and commercial relationships. These include:

- the members of the General Assebly of the Members;
- the members of the Coordination and Management Committee;
- the President and Vice-President of the Association;
- the members of the Scientific and Steering Committee;
- the members of the Control Body;
- the members of the Supervisory Body;
- personnel
- collaborators and consultants;
- commercial partners;
- customers and/or served companies;
- suppliers of goods and services, continuous or occasional;
- anyone who, for any reason or activity, operates in the interest, in the name, and on behalf of the Association or maintains relationships of any nature with it.

In the following, for reasons of brevity, the above-identified parties will be referred to simply as the "Recipients"

Knowledge and observance of the Code of Ethics represent an indispensable requirement for establishing and maintaining relationships with the Association and primary conditions for the good reputation and image of Cyber 4.0.

### 2.2 Communication and Dissemination of the Code

In relation to the Code of Ethics, Cyber 4.0 ensures:

- Periodic reviews and updates, to ensure that the Code is always aligned with the evolution of the Association and remains fully compliant with applicable regulations;
- Dissemination, through publication on the corporate website www.cyber40.it, illustration of its contents, and delivery of an updated copy to all employees, whether already employed at the time of the Code's approval or newly hired;
- A periodic information and training program for the Recipients, regarding the content and significance of the Code of Ethics;
- Full confidentiality and professional protection for anyone who needs to report potential violations of the Code, without prejudice to legal obligations.

## 3. General Principle

### 3.1 Introduction

The Association has decided to formalize the principles to which it recognizes a positive, primary, and absolute ethical value. These principles represent the fundamental values that all individuals bound to comply with the Code of Ethics must adhere to in pursuing the corporate mission and, more generally, in the conduct of the Association's activities.

### 3.2 Professionalism

Professionalism, dedication to assigned tasks, and mutually supportive behavior constitute key values for achieving the Association's objectives.

For this reason, Cyber 4.0 fosters the development of its employees' professional skills, implements policies that recognize and enhance individual merit, and operates in full compliance with equal opportunity

principles. Each employee must act with commitment and ethical rigor, safeguarding, under all circumstances, the image and good reputation of Cyber 4.0.

### 3.3 Impartiality and Non-Discrimination

In decisions affecting its relationships with stakeholders, Cyber 4.0 rejects any form of discrimination based, among other factors, on gender, age, disability, nationality, sexual orientation, ethnicity, religion, or political opinions.

### 3.4 Legality, Honestly and trasparency

In the context of their professional activities and relationships with stakeholders, the Recipients of this Code – in the performance of their functions and duties – are required to comply diligently, honestly, and transparently with applicable laws at the national, European, and international levels, national and European decrees and regulations, the Code of Ethics, the 231 Model, the Association's policies, and the entire internal regulatory system adopted by the Association.

Under no circumstances can the pursuit of Cyber 4.0 interests justify conduct that constitutes a violation of applicable laws or that, in any case, is inconsistent with the principles expressed herein.

### 3.5 Valuing people

Cyber 4.0, being aware of the importance and centrality of human resources for the development of its activities and the achievement of its corporate objectives, protects and promotes the professional growth of its employees, aiming to enhance and expand their knowledge and skills.

### 3.6 Fairness in Relationships with Subordinates

In contractual relationships where hierarchical structures exist among its personnel,Cyber 4.0 commits to ensuring that authority derived from positions of seniority is exercised while avoiding and rejecting any form of abuse and without undermining, in any way, the personal and professional dignity of its employees.

### 3.7 Protection of Health and Workplace Safety

The Association is fully committed to ensuring the health and safety of the workplace.

### 3.8 Environmental Protection

Cyber 4.0 is committed to operating in respect of the environment and the health of individuals, fully aware of its social and ethical responsibilities toward the communities in which it operates or from which it draws resources.

### 3.9 Quality of services and products

Cyber 4.0 directs its activities toward the satisfaction and protection of both its clients and its members, taking into account and responding to requests and suggestions that may contribute to improving the quality of the services offered, in order to achieve the social objectives.

### 3.10 Fair Competition

The Association recognizes the value of fair competition as a tool for the efficient allocation of society's resources and is committed to refraining from collusive or exploitative behavior and from abusing any dominant positions. Recipients are required to comply with all applicable laws safeguarding fair trade and to abstain from actions that could lead to unfair commercial practices, which could result in liability for the Association in any capacity.

### 3.11 Protezione dei dati personali

Cyber 4.0 complies with the provisions regarding the protection of personal data set forth in Legislative Decree no. 196 of 2003, as amended by EU Regulation no. 2016/679 and Legislative Decree 101/2018, governing the "Personal Data Protection Code" and subsequent amendments and integrations, as well as the relevant implementing regulations.

The Association is committed to protecting privacy and ensuring the confidentiality of personal data of Recipients that it comes into possession of in the course of its activities, in compliance with applicable laws.

To this end, Cyber 4.0 has implemented internal procedures to regulate the Association's communication activities, including from the perspective of personal data protection and the security of applications, and is committed to carrying out ongoing updates and reviews to ensure their compliance with current laws and alignment with changes in the Association's activities.

Cyber 4.0 has also obtained certifications according to the UNI ISO 9001:2015 standard (Quality Management Systems – Requirements) and UNI ISO 27001:2022 (Information Security, Cybersecurity and Privacy Protection – Information Security Controls).

### 3.12 Diligence and Fairness in the Execution of Contracts

Cyber 4.0 respects the duties and obligations arising from contracts entered into with members, clients/served companies, and suppliers, which must be fulfilled with the diligence of a prudent person and in accordance with what has been consciously agreed upon by the parties, avoiding abuses resulting from the ignorance and/or incapacity of its counterparts. Moreover, Cyber 4.0 is committed not to take advantage of contractual gaps or specific events to renegotiate, due to its dominant position and/or the counterpart's weakness, contractual conditions in order to obtain undue or unwarranted benefits of any kind, including non-financial advantages.

### 3.13 Diligence, Fairness, and Transparency in Fulfilling Obligations Arising from Relations with Public Administrations and Other Public Entities

Cyber 4.0 respects – aligning its actions with the principles of diligence, fairness, and transparency – the duties and obligations arising from agreements and other equivalent acts entered into with national or European Public Administrations and Public Entities in order to achieve the social objectives.

The same principles must be observed by the Recipients whenever, by virtue of their role or specific authorizations, they interact or have contacts, in the name and on behalf of the Association, with such bodies and with public officials or individuals entrusted with a public service.

### 3.14 Prevention of Conflicts of Interest

The Association's personnel are required to perform their work with diligence, competence, and loyalty, refraining from promoting or otherwise participating in initiatives that could place them in a situation of conflict of interest with the Association or its stakeholders, whether on their own behalf or on behalf of third parties.

A conflict of interest shall be understood, in addition to what is provided for by law, as both a situation in which an individual holds or pursues – on their own behalf or on behalf of third parties – a commercial, financial, and/or personal interest that is distinct from and incompatible with the corporate objectives of Cyber 4.0, and a situation in which representatives of clients or suppliers act, in the context of contractual relationships with the Association, in conflict with the fiduciary duties related to their position.

In the event that a conflict of interest exists or may arise, Recipients are required to promptly inform the Association and/or the Supervisory Body.

### 3.15 AI & Cybersecurity

Cyber 4.0 considers cybersecurity and the ethical and responsible use of Artificial Intelligence as inseparable safeguards of legality, reliability, and sustainability of its business model, as well as essential components of the risk prevention system pursuant to Legislative Decree No. 231/2001.

In line with these principles, the Association undertakes to ensure full compliance with applicable national and supranational legislation, as well as with international best practices in the fields of Artificial Intelligence governance and the security of networks and information systems.

Cyber 4.0 promotes the use of Artificial Intelligence based on principles of responsibility, transparency, and respect for fundamental human rights. From this perspective, the testing, development, adoption, and deployment of AI systems and models must comply with applicable laws and regulations, principles of professional integrity, and values safeguarding human dignity.

The Association acknowledges that Artificial Intelligence may have a significant impact on the legal and social sphere of individuals and undertakes to prevent uses of algorithmic systems that may lead to discrimination, unfair treatment, undue restrictions of rights, decision-making opacity, or adverse effects on personal autonomy and human dignity.

The use of AI-based technological solutions is assessed with regard to ethical considerations, security-related risks, the protection of personal data, and impacts on decision-making processes. Finally, the Association ensures that such systems are employed as support tools and not as substitutes for professional judgment, in compliance with the necessary safeguards of human oversight.

To this end, Cyber 4.0 provides adequate information on the operating methods of AI products, as well as on the risks arising from the use of artificial intelligence systems.

The Association undertakes to ensure compliance with Regulation (EU) 2024/1689 (hereinafter, the “AI Act”) and with the applicable national legislation on artificial intelligence (Law No. 132/2025), throughout the entire lifecycle of the products. In this respect, Cyber 4.0:

- respects human dignity and individual autonomy;
- safeguards the rights and freedoms of individuals;
- ensures transparency in its operations;
- continuously supervises the functioning of robotic and AI systems;
- seeks to prevent errors and “hallucinations” through validation and control mechanisms;
- prohibits any form of inequality or discrimination;
- protects privacy and personal data;

- ensures the adoption of appropriate cybersecurity measures;
- manages suppliers and external models/services, including compliance checks and contractual clauses consistent with the Organisational, Management and Control Model pursuant to Legislative Decree No. 231/2001;
- organises periodic training programmes and promotes AI literacy.

The Association recognises cybersecurity as a foundational value of its activities and as an essential prerequisite for building trust with customers, partners, institutions, and the market. The protection of systems, data, and digital infrastructures constitutes a shared responsibility and a duty of all Recipients of this Code.

Each Recipient, in relation to their role, functions, and assigned powers, is required to use IT resources diligently and in compliance with internal policies, to contribute to the prevention of incidents, to promptly report events, anomalies, or vulnerabilities, and to refrain from any conduct that may compromise the security, integrity, confidentiality, or availability of information and systems.

The Association further undertakes to promote and maintain an adequate level of awareness by establishing periodic training and update programmes in the field of cybersecurity and by ensuring their effective participation by the Recipients, in line with their respective roles and responsibilities.

## 4. Code of conduct

### 4.1 Criteria of Conduct for Corporate Bodies

Members of the corporate bodies, by virtue of their fundamental role, are required to comply with the provisions of the 231 Model and the Code of Ethics, performing their duties with seriousness, professionalism, and in accordance with the principles of legality, honesty, and fairness.

The corporate bodies must act in a responsible and loyal manner toward the Association, the other members, and stakeholders and, upon prior notification to the Administrative Body, must refrain from performing acts in the presence of an actual or potential conflict of interest. They must also make confidential use of, and in any event not disclose, information acquired by virtue of their office

### 4.2 Criteria of conduct toward members

Cyber 4.0 considers it to be in its specific interest to ensure a continuous and open relationship, based on mutual understanding of roles, with all members of the Association—whether public or private—by

grounding interactions on principles of fairness, honesty, transparency, and loyal cooperation, in line with international best practices.

### 4.3 Criteria of Conduct in Personnel Selection

The recruitment and selection of personnel are carried out solely on the basis of the alignment between candidates' profiles and the expected requirements and professional needs of the Association, according to objective and transparent criteria, in compliance with the principles of equal opportunity, avoiding any form of favoritism or discrimination.

The information requested during the recruitment process concerns the assessment of professional and psycho-aptitudinal aspects—while respecting the dignity, privacy, and opinions of candidates—and is stored and processed in compliance with applicable regulations on the protection and confidentiality of personal data, for the time strictly necessary for the purposes of processing.

### 4.4 Criteria of Conduct in Relations with Personnel and Collaborators

Human capital is a fundamental factor for the development and growth of the Association.

Personnel management is characterized by strong attention to all actions that may contribute to creating, for its employees, not only adequate financial remuneration but also improved personal and family life conditions.

The well-being of individuals who work for or within the Association is also achieved through constant attention to the work environment and organization, in which smart working arrangements have been enhanced, as well as through mutual solidarity and any initiative capable of fostering cohesion, corporate identity, and the enhancement of diversity.

### 4.5 Criteria of Conduct in Relations with Clients

Contracts with clients must comply with applicable laws and must be defined in a clear and comprehensive manner. In their relations with clients, employees must adopt a courteous and cooperative attitude, safeguarding the corporate image to the greatest extent possible and respecting the principles of impartiality and non-discrimination.

### 4.6 Criteria of Conduct in Relations with Suppliers

The procurement processes for goods or services are guided by the utmost transparency, efficient allocation of resources, the pursuit of the best economic and competitive advantage for the Association, as well as prior and traceable verification that suppliers—whether members or non-members—meet specific professional, reputational, and legal requirements, including, where applicable, authorization to carry out the relevant

activity or profession. Contractual and pre-contractual relationships between the Association and suppliers are based on principles of mutual loyalty, transparency, and cooperation.

In external collaboration relationships (including consultants), the personnel involved are required, by virtue of specific contractual clauses, to formally adhere to the principles set forth in the 231 Model and in this Code of Ethics adopted by Cyber 4.0, as well as to comply with applicable laws and regulations.

**4.7 Criteria of Conduct in Relations with Public Administrations and Public Bodies (National or Supranational)**

In its relations with Public Administrations and/or Public Bodies (national or EU-level), Cyber 4.0 undertakes to comply with the obligations assumed, arising from the agreements entered into, the role it holds, and its core business, as provided for by the applicable laws in force from time to time, ensuring that such obligations are fulfilled correctly and in a timely manner, in accordance with the principles of transparency, honesty, and loyal cooperation.

In line with the same obligations, the Association is committed to ensuring the accuracy, truthfulness, and reliability of data and information whose communication and/or transmission, in any form, is required in favor of the relevant Public Administrations and Public Bodies.

To this end, Cyber 4.0 has adopted an internal regulatory framework to govern the fulfillment of communication and reporting obligations toward Public Administrations and Public Bodies (national and EU-level), providing that only duly authorized individuals may maintain relationships or contacts with institutional counterparts. The Association also undertakes to carry out ongoing updates and revisions of such framework in order to ensure compliance with the laws in force from time to time and alignment with changes in the Association's activities.

**4.7 Relation with Press and Media**

External communication, whether with the press or other media outlets, must always be truthful and transparent and must preserve the reputation of the Association through the accurate dissemination of implemented programs and achieved performance.

Relations with representatives of the media are reserved exclusively to the designated function.

**5. Confidentially**

Cyber 4.0 ensures and guarantees the confidentiality of the information in its possession.

Employees of Cyber 4.0 are required to maintain the confidentiality of any news and/or information of a confidential nature acquired from members, clients, suppliers, or otherwise obtained by virtue of their role, in order to ensure the highest level of confidentiality regarding the Association's documents and information

(including projects, proposals, strategies, negotiations, understandings, commitments, and contracts in the process of being finalized).

**6. Prevention of Corruption and Fraud**

Cyber 4.0 does not tolerate any form of fraud or corruption, whether active or passive, including private-to-private corruption, illicit influence trading, and the granting of advantages or incentive payments. In particular, by way of example and not limitation, it prohibits any action by or towards third parties aimed at promoting or favoring its own interests or deriving benefits therefrom. Furthermore, it does not permit the offering of money, other benefits, or advantages to individuals who are part of, or connected to, Public Administrations or the corporate structures of third parties in order to obtain contracts or any other advantage for the Association.

Cyber 4.0 is committed to implementing all necessary measures to prevent and avoid corruption, fraud, and money laundering; to this end, every action, operation, transaction, and accounting entry must be conducted with the utmost fairness, completeness, transparency, and truthfulness.

**6.1 Sponsorship, gift and other benefits**

The Association prohibits any improper use of sponsorships, donations, gifts, or other benefits that could even be interpreted as exceeding normal commercial or courtesy practices, or as instrumental in obtaining preferential treatment related to activities of the Association in favor of public officials, individuals entrusted with a public service, their family members, or private parties that maintain any type of commercial or economic relationship with the Association.

The same conduct rules apply both to gifts or benefits offered by the Recipients of this Code of Ethics and to gifts or benefits received by them.

Any Recipient who has even the slightest suspicion or doubt regarding the offering or receipt of undue gifts or benefits must immediately report it to their Supervisor/Hierarchical Superior, to the Association, and/or to the Supervisory Body.

**7. Accounting integrity**

Cyber 4.0 pursues and ensures the completeness, accuracy, and reliability of the information necessary for the preparation of any disclosure attributable to the Association, also in compliance with the standards governing the preparation and maintenance of internal accounting records and their external disclosure in accordance with the applicable legislation in force from time to time.

Personnel are required to provide the utmost cooperation to ensure that management events are correctly and promptly recorded within the Association's accounting and reporting system.

**8. Protection of Corporate Assets and Information Security**

Each Recipient is required to use any corporate assets made available to them, where applicable, in accordance with principles of the utmost diligence, good faith, and fairness, and in compliance with the purposes for which such assets have been granted.

It is strictly prohibited to use corporate assets for personal purposes or to use one's role and/or information acquired in the performance of one's duties to pursue personal and/or family interests. With reference to the use of IT tools, and in particular email services and internet access, conduct must be guided by principles of loyalty and fairness and must comply with the regulations set forth by the applicable laws in force from time to time, as well as by the policies, internal procedures, and operating instructions adopted by the Association, which are continuously updated and reviewed to ensure compliance with current legislation and alignment with changes in the Association's activities.

**9. Implemetation of Code of Ethics**

**9.1 Criteria for the application and implementation**

Cyber 4.0 undertakes to disseminate the principles and obligations set forth in this document to all Recipients, so that each individual adopts conduct inspired by ethics, honesty, fairness, and professionalism, aimed at ensuring the quality of services provided, respect for the environment, and the health and safety of workers, as well as the highest level of customer satisfaction and the broader needs of users of the products and services delivered.

For this reason, in accordance with the Association's Statute, the Cyber 4.0 Control and Management Committee adopts the appropriate resolutions and initiatives to ensure the full application and implementation of the Code of Ethics.

It is the responsibility of the Supervisory Body to monitor compliance with the provisions contained in this Code of Ethics and to propose any amendments or additions, submitting them to the attention of the Control and Management Committee for the necessary approval.

### 9.2 Violation of the Code of Ethics: Reporting Procedures and Sanctioning System

Any violation of the provisions contained in this Code of Ethics constitutes a disciplinary offense, subject to sanctions pursuant to applicable law and/or the relevant National Collective Bargaining Agreement (CCNL), and, with regard to external collaborators, a contractual breach.

Decisions and conduct in violation of this Code shall not be tolerated by the Association under any circumstances.

Any violation of the principles and provisions set forth in this Code of Ethics must be promptly reported by the Recipients to the Reports Manager, in order to benefit from the protections provided under the applicable whistleblowing legislation.

Cyber 4.0 has adopted a procedure for the management of reports, available on the Association's website at the following link: https://cyber40.segnalazioni.net. It has also established an internal reporting channel (so-called "whistleblowing") that allows reporters to submit reports in accordance with the protection system provided by Legislative Decree no. 24/2023, and has designated the Supervisory Body as the Reports Manager, endowed with the necessary autonomy, independence, and professionalism.

The implemented platform,Legality Whistleblowing by Digital PA, complies with the requirements set forth in Legislative Decree no. 24/2023 and is accessible through the Association's website at www.cyber40.it.

Cyber 4.0 ensures protection for reporting persons against any form of retaliation and does not allow the adoption of any disciplinary and/or sanctioning measures for reports made in good faith.

Where reports received require confidential handling, in compliance with applicable regulations, the Association undertakes to safeguard such confidentiality, without prejudice to statutory provisions, the applicable CCNL, and any regulations or procedures relevant to the specific case.