applied®

# Suppliers code of conduct

6. Quality, innovation and professionalism

7. Environmental sustainability and corporate social responsibility

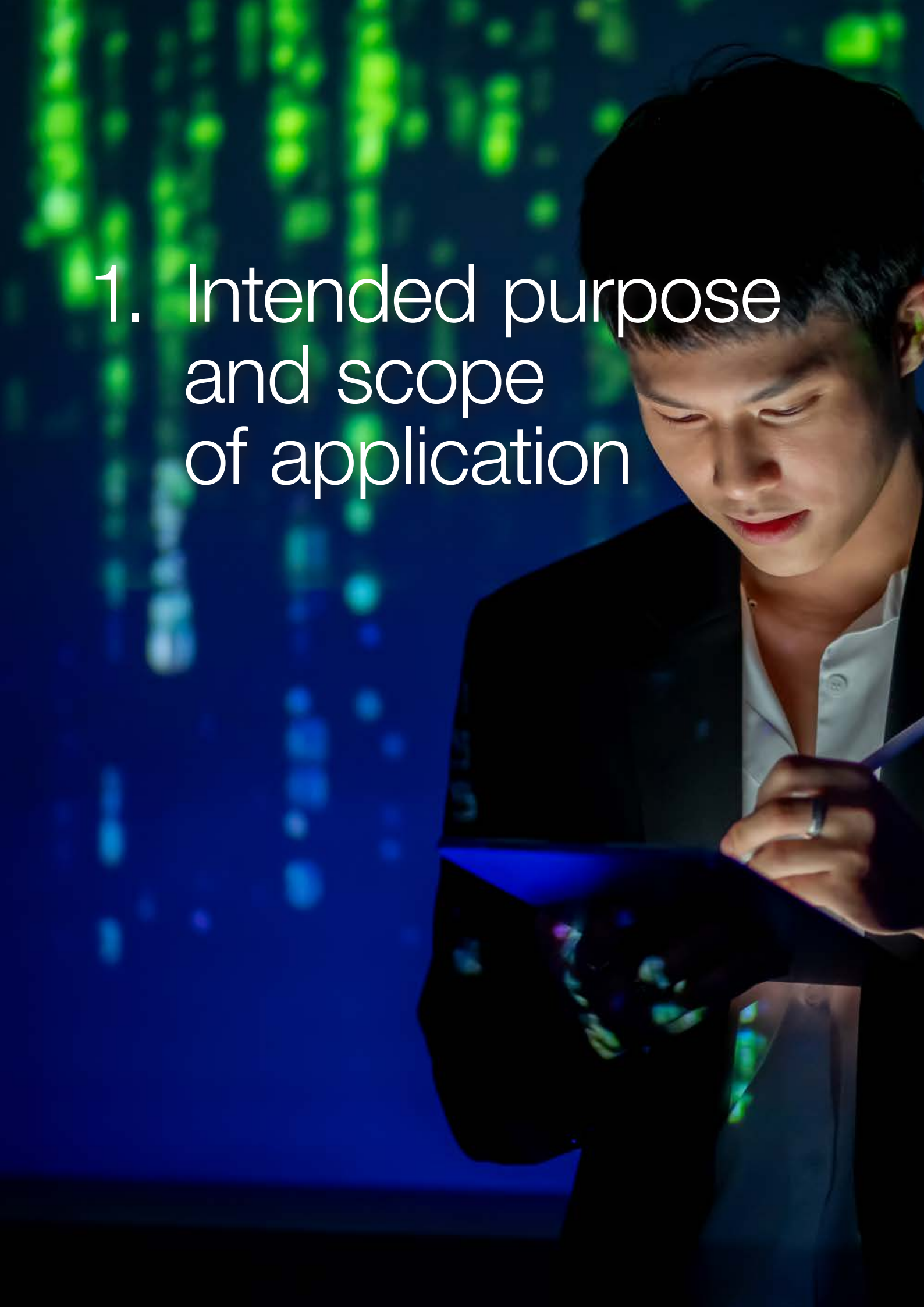
8. Code of ethics in artificial intelligence and the use of algorithms

9. Reporting and whistleblowing

10. Monitoring, auditing and related implications

11. Supplier's, binding commitment

12. Updates and disclosure



# 1. Intended purpose and scope of application

# 1.0
# INTENDED PURPOSE AND SCOPE OF APPLICATION

This Supplier Code of Conduct establishes the **ethical, social, environmental, quality and safety standards** that the Applied Group requires from all its suppliers, partners and sub-suppliers.

The aim is to ensure that the entire supply chain operates in a transparent, responsible and sustainable manner, reflecting the core values expressed in the **Company's Code of Ethics (APPL-COMPL-PL-001).**

Adherence to the Code is a **binding commitment for every supplier** and an essential condition for establishing and maintaining business relationships with Applied.

# 2. Core principles

## 2.1 INTEGRITY AND TRANSPARENCY

Suppliers must conduct their business with **fairness, professionalism and loyalty.**

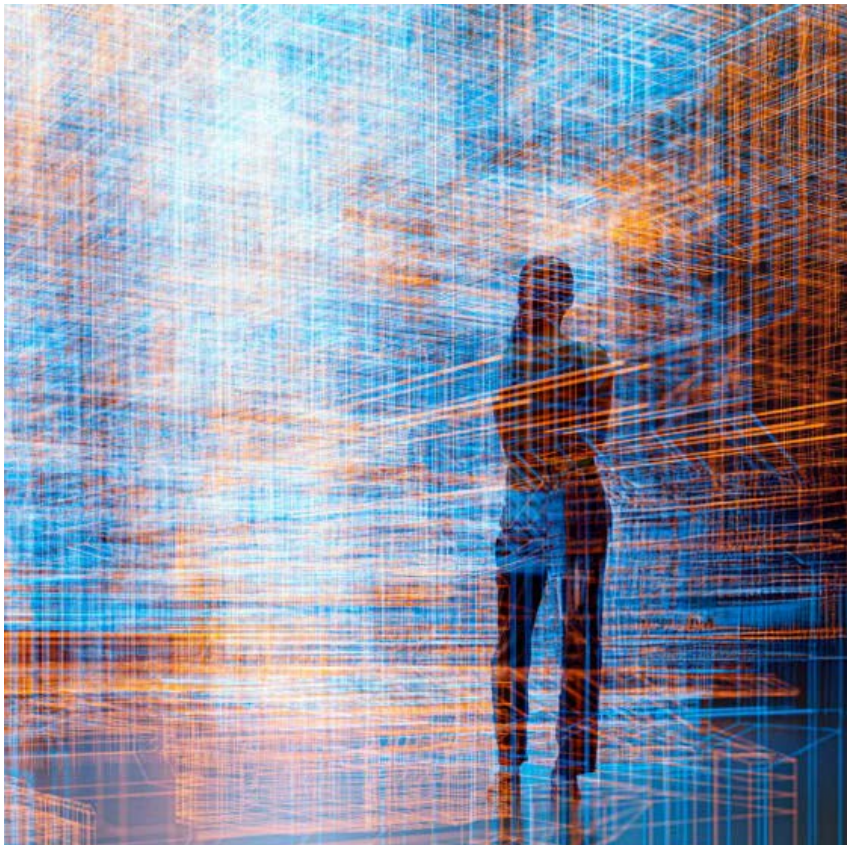
Any form of corruption, extortion, fraud, abuse of power or illegal practice that could compromise trust in commercial relationships is prohibited. In particular:

- No gifts, benefits or advantages of non-symbolic value that could influence business decisions may be offered or accepted. Any gifts must be **occasional, proportionate and traceable.**
- Any conflicts of interest, even potential ones, must be **disclosed and managed transparently**, avoiding situations that could compromise the impartiality of decisions.
- Unfair competition practices, collusive agreements, signs or behaviour that damage the reputation of the Applied Group are prohibited.

## 2.2 OBSERVANCE OF HUMAN RIGHTS AND WORKING CONDITIONS

Suppliers must ensure that every worker is treated with **dignity, fairness and respect.**

- The use of child labour, forced or compulsory labour, including human trafficking or debt obligations, **is strictly prohibited.** All employment relationships must be **voluntary and freely chosen.**
- The rights of trade union membership and collective bargaining must be respected.
- Workers must receive **wages and working hours in accordance with the law**, holidays, rest periods and fair conditions of employment.
- Workplaces must be safe, healthy and comply with health and safety regulations. Prevention programmes, regular training and emergency plans must be in place.
- Any form of **harassment, abuse, discrimination or intimidation** must be prevented, promoting a collaborative and inclusive environment.



## 2.3
## DIVERSITY AND INCLUSION

Applied values diversity and requires suppliers to:

- Ensure equal opportunities without discrimination based on gender, age, ethnicity, religion, sexual orientation, disability or personal opinions.
- Value the diversity of skills and experiences as a lever for innovation and collective growth.

# 3. Legal and regulatory compliance

# 3.0
# LEGAL AND REGULATORY COMPLIANCE

All suppliers must operate in compliance with applicable local, national and international laws and regulations. This includes, but is not limited to:

- Tax, customs and trade regulations;
- Labour and social security legislation;
- Competition and anti-corruption regulations;
- Personal data protection regulations (GDPR);
- NIS2 Directive for cyber security and AI Act for artificial intelligence, where applicable.

Any regulatory violations by the supplier must be reported to Applied promptly.

# 4. Confidentiality, GDPR and Data Protection

## 4.1
## ETHICAL MANAGEMENT AND INFORMATION CONFIDENTIALITY

Applied's confidential information (technical, commercial, financial, personal data) must be treated as **strictly confidential.** Any misuse or unauthorised disclosure is prohibited. Access must be limited to authorised personnel and only for purposes strictly related to the contractual relationship.

## 4.2
## DATA PROCESSING SECURITY

Suppliers must comply with the GDPR principles: lawfulness, fairness, minimisation, accuracy, storage limitation and protection from unauthorised access.

They must implement appropriate technical and organisational measures, including encryption, multi-factor authentication, access controls and anomaly monitoring.

In the event of a violation or suspected data breach, the supplier is required to notify Applied promptly and cooperate to mitigate the risks.

# 5. Cyber security and business continuity

# 5.1
# SECURITY MANAGEMENT SYSTEM

Suppliers are required to adopt robust IT security policies and implement a consistent set of technical, organisational and procedural measures appropriate to the level of risk. These measures must be based on widely recognised international standards and best practices, such as those described in ISO/IEC 27001.

In particular, suppliers must:

- **Proactively manage vulnerabilities** by ensuring regular updates and patches to systems, applications and devices;
- **Ensure continuous monitoring** of infrastructure and services in order to detect incidents or anomalous behaviour in a timely manner;
- Apply network segmentation to limit the impact of any compromises and improve the isolation of critical systems;
- Protect data through encryption, both during transmission and storage, using recognised and secure algorithms and protocols;
- Define and implement organisational procedures for managing security incidents, with clearly identified roles and responsibilities;
- Train and raise awareness among personnel on cyber risks and good security practices, on an ongoing and up-to-date basis;
- Implement access controls based on the principle of least privilege and strong authentication mechanisms;
- Conduct periodic checks and audits to assess the effectiveness of the measures taken and identify areas for improvement.

The objective is to ensure an adequate and constantly evolving level of protection, capable of countering increasingly sophisticated cyber threats and effectively safeguarding company data, systems and processes.

## 5.2
## INCIDENT RESPONSE AND BUSINESS CONTINUITY

Each supplier must have **a structured plan to address cybersecurity incidents**, including clear and formalised procedures for:

- **Timely identification** of threats, anomalies and potential incidents through monitoring, detection and reporting systems;
- **Classification and assessment** of incidents based on severity, impact and urgency, using pre-established criteria;
- **Immediate containment** to limit the spread of the attack and reduce damage to systems and data;
- **Technical resolution and restoration** of compromised systems, ensuring full operation of the infrastructure and applications involved;
- **Internal and external communication**, including notification to the client within defined timescales and, if required, to the competent authorities;
- **Post-incident analysis** to identify root causes, define corrective actions and prevent similar events from recurring.

In addition, each supplier must prepare and maintain a **Business Continuity Plan (BCP)** and a **Disaster Recovery Plan (DRP)** to ensure the provision of services even in the event of critical events (e.g. infrastructure failures, ransomware attacks, natural disasters).

# 6. Quality, innovation and professionalism

# 6.0
# QUALITY, INNOVATION AND PROFESSIONALISM

Suppliers are fully responsible for the **quality of the products and services** they provide to Applied. This implies the adoption of high standards throughout the entire supply lifecycle, with particular attention to:

- **Technical accuracy and reliability**: products and services must comply with technical specifications, regulatory and contractual requirements, and guarantee consistent and verifiable performance.
- **Quality control processes**: suppliers must implement structured control and monitoring systems, including periodic tests, checks and audits, to ensure compliance with agreed service levels.
- **Traceability and documentation**: each supply must be accompanied by complete, transparent and accurate documentation (manuals, certifications, test reports, technical data sheets) to demonstrate the conformity of the product/service.
- **Staff professionalism**: the staff involved must have adequate, up-to-date and certified skills, as well as maintaining high standards of professional ethics and responsibility.

Applied also encourages suppliers to promote **technological and methodological innovation**, provided that it is developed and adopted in accordance with the following principles:

- **Ethics and responsibility**: innovations must guarantee safety, transparency and compliance with current regulations.
- **Sustainability**: every new process, methodology or technology must be assessed in terms of its environmental and social impact, favouring low-impact and energy-efficient solutions.
- **Security**: the adoption of new technologies must always include a risk analysis and the introduction of adequate protection measures for users, data and infrastructure.

# 7. Environmental sustainability and corporate social responsibility

# 7.0 ENVIRONMENTAL SUSTAINABILITY AND CORPORATE SOCIAL RESPONSIBILITY

Suppliers must contribute to reducing the environmental impact of their activities by:

- reducing energy and water consumption;
- responsible waste management and proper disposal of WEEE;
- use of renewable energy sources;
- promotion of low-impact working models (e.g. smart working, remote meetings).

They must also support social and community initiatives, promoting ethical behaviour throughout the supply chain.

# 8. Code of ethics in artificial intelligence and the use of algorithms

# 8.0
# CODE OF ETHICS IN ARTIFICIAL INTELLIGENCE AND THE USE OF ALGORITHMS

When developing or using AI systems, suppliers must ensure

- **Transparency** of algorithms, which must be documented and explainable;
- **Reliability and constant monitoring** of solutions;
- **Human responsibility in critical decisions;**
- **Fairness** and prevention of discrimination;
- **Security** of algorithms against abuse or attacks.

# 9. Reporting and Whistleblowing

# 9.0
# REPORTING AND WHISTLEBLOWING

Applied has established a whistleblowing channel that is also accessible to suppliers, allowing them to report violations or unlawful conduct. The channel can be found on the corporate website **www.applied.it** .

Reports are treated confidentially, ensuring the protection of the whistleblower's identity and protection from retaliation.

Suppliers are required to cooperate in investigations and implement any corrective actions.

# 10. Monitoring, auditing and related implications

# 10.0
# MONITORING, AUDITING AND RELATED IMPLICATIONS

Applied reserves the right to verify compliance with the Code through audits, inspections and requests for documentation.

In the event of violations:

- immediate corrective action may be required;
- collaboration may be suspended until compliance is restored;
- in serious or repeated cases, the contract may be terminated.

# 11. Supplier's binding commitment

# 11.0
# SUPPLIER'S BINDING COMMITMENT

By signing the contract or commencing work, the supplier formally declares that they:

- have read, understood and accepted this Code of Conduct;
- undertake to comply with it in its entirety;
- will disseminate its contents within their organisation and supply chain;
- actively cooperate with Applied in the event of audits or requests for corrective action;
- promptly report any violations.

# 12. Updates and disclosure

# 12.0
# UPDATES AND DISCLOSURE

This Code is subject to periodic revisions in line with regulatory and technological developments and business needs.

Updated versions will be communicated to all suppliers and published on Applied's corporate website so that they are always accessible and available for consultation.

| | |
|---|---|
| Società di riferimento | **APPLIED** |
| Perimetro di validità | Aziende gruppo Applied |
| Ambito documento | COMPLIANCE |
| Codificazione | APPL-COMPL-PL-002 |
| Nome esteso documento | APPL-COMPL-PL-002-Codice di Condotta Fornitori-v01 |
| Documento | Codice di Condotta Fornitori |
| Versione | 1 del 01/10/2025 |
| Lingua | Inglese |
| Approvatore | Head of Staff |
| Autore | Cyber Security & Compliance Manager |
| Data di approvazione | 01/10/2025 |
| Data classification | Pubblico |


applied®
innovation makers