applied®

Codice condotta fornitori

6. Qualità, innovazione e professionalità

7. Sostenibilità ambientale e responsabilità sociale

8. Etica nell'intelligenza artificiale e nell'uso degli algoritmi

9. Segnalazioni e Whistleblowing

10. Monitoraggio, auditel e conseguenze

11. Impegno vincolante del fornitore

12. Aggiornamenti e diffusione

1. Scopo e campo di applicazione

1.0
MISSIONE E VISIONE

Il presente Codice di Condotta Fornitori stabilisce gli **standard etici, sociali, ambientali, di qualità e di sicurezza** che il Gruppo Applied richiede a tutti i propri fornitori, partner e subfornitori.

L'obiettivo è garantire che l'intera catena di fornitura operi in modo trasparente, responsabile e sostenibile, riflettendo i valori fondamentali espressi nel **Codice Etico aziendale (APPL-COMPL-PL-001).**

L'adesione al Codice costituisce **impegno vincolante per ogni fornitore** e condizione imprescindibile per instaurare e mantenere rapporti commerciali con Applied.

2. Principi fondamentali

2.1 INTEGRITÀ E TRASPARENZA

I fornitori devono condurre i propri affari con correttezza, professionalità e spirito di lealtà.

È vietata qualsiasi forma di corruzione, concussione, frode, abuso di potere o pratica illecita che possa compromettere la fiducia nei rapporti commerciali.

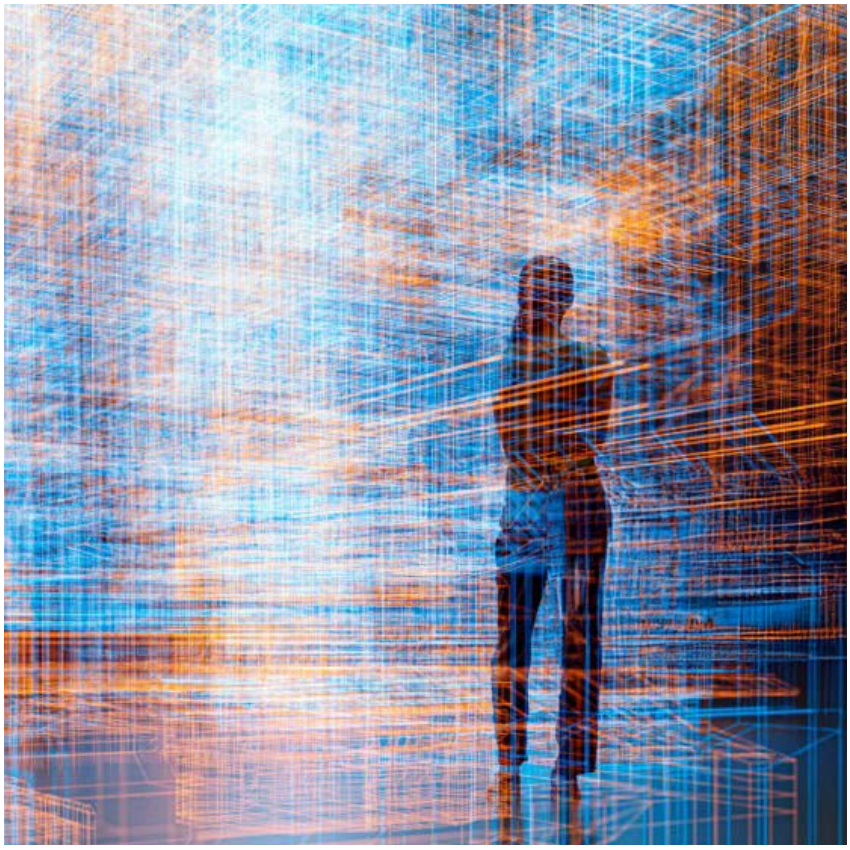
In particolare:

- Non devono essere offerti né accettati regali, benefici o vantaggi di valore non simbolico, che possano influenzare decisioni aziendali. Qualsiasi omaggio deve essere **occasionale, proporzionato e tracciabile.**
- Eventuali conflitti di interesse, anche potenziali, devono essere **dichiarati e gestiti con trasparenza**, evitando situazioni che possano compromettere l'imparzialità delle decisioni.
- Sono vietate pratiche di concorrenza sleale, accordi collusivi, cartelli o comportamenti che danneggino la reputazione del Gruppo Applied.

2.2 RISPETTO DEI DIRITTI UMANI E CONDIZIONI DI LAVORO

I fornitori devono garantire che ogni lavoratore sia trattato con dignità, equità e rispetto.

- È fatto assoluto divieto di ricorrere a lavoro minorile, forzato o coatto, inclusi traffico di esseri umani o vincoli di debito. Tutti i rapporti di lavoro devono essere volontari e liberamente scelti.
- Devono essere rispettati i diritti di associazione sindacale e di contrattazione collettiva.
- I lavoratori devono beneficiare di retribuzioni e orari conformi alla legge, ferie, riposi e condizioni eque di impiego.
- Gli ambienti di lavoro devono essere sicuri, salubri e conformi alle normative in materia di salute e sicurezza. Devono essere predisposti programmi di prevenzione, formazione periodica e piani di emergenza.
- È necessario prevenire qualsiasi forma di molestia, abuso, discriminazione o intimidazione, promuovendo un clima di collaborazione e inclusione.
- L'azienda incoraggia la pluralità di esperienze e punti di vista come elemento di innovazione e crescita collettiva.



2.3
DIVERSITÀ E INCLUSIONE

Applied considera la diversità un valore e richiede ai fornitori di:

- Garantire pari opportunità senza discriminazioni basate su genere, età, etnia, religione, orientamento sessuale, disabilità o opinioni personali.
- Valorizzare la pluralità di competenze ed esperienze come leva di innovazione e crescita collettiva.

3. Conformità legale e regolatoria

3.0
CONFORMITÀ LEGALE E REGOLATORIA

Tutti i fornitori devono operare nel rispetto delle leggi e normative vigenti a livello locale, nazionale e internazionale. Questo include, a titolo esemplificativo:

- Norme fiscali, doganali e commerciali;
- Legislazione sul lavoro e sicurezza sociale;
- Normativa in materia di concorrenza e anticorruzione;
- Normativa sulla protezione dei dati personali (GDPR)
- Direttiva NIS2 per la cyber security e l'AI Act per l'intelligenza artificiale, ove applicabili.

Qualsiasi violazione normativa da parte del fornitore deve essere comunicata tempestivamente ad Applied.

4. Riservatezza, GDPR e protezione dei dati

4.1
GESTIONE ETICA E RISERVATEZZA DELLE INFORMAZIONI

Le informazioni riservate di Applied (dati tecnici, commerciali, finanziari, personali) devono essere trattate come strettamente confidenziali.

È vietato qualsiasi uso improprio o divulgazione non autorizzata. L'accesso deve essere limitato al personale autorizzato e solo per finalità strettamente connesse al rapporto contrattuale.

4.2
SICUREZZA NEL TRATTAMENTO DEI DATI

I fornitori devono rispettare i principi del GDPR: liceità, correttezza, minimizzazione, accuratezza, limitazione della conservazione e protezione da accessi non autorizzati.

Devono implementare misure tecniche e organizzative adeguate, tra cui crittografia, autenticazione a più fattori, controlli sugli accessi e monitoraggio delle anomalie.

In caso di violazione o sospetto data breach, il fornitore è tenuto a notificare Applied entro tempi rapidi e a collaborare per mitigare i rischi.

5. Cyber security e continuità operativa

5.1 SISTEMA DI GESTIONE DELLA SICUREZZA

I fornitori sono tenuti ad adottare politiche di sicurezza informatica robuste e a implementare un insieme coerente di misure tecniche, organizzative e procedurali adeguate al livello di rischio. Tali misure devono ispirarsi a standard e best practice internazionali ampiamente riconosciuti, come quelli descritti dalla norma ISO/IEC 27001.

In particolare, i fornitori devono:

- **Gestire in modo proattivo le vulnerabilità**, garantendo aggiornamenti e patch regolari dei sistemi, applicazioni e dispositivi;
- **Assicurare il monitoraggio continuo** delle infrastrutture e dei servizi, al fine di rilevare tempestivamente incidenti o comportamenti anomali;
- **Applicare la segmentazione delle reti** per limitare l'impatto di eventuali compromissioni e migliorare l'isolamento dei sistemi critici;
- **Proteggere i dati tramite crittografia**, sia durante la trasmissione sia nella fase di archiviazione, con algoritmi e protocolli riconosciuti come sicuri;
- **Definire e attuare procedure organizzative** per la gestione degli incidenti di sicurezza, con ruoli e responsabilità chiaramente individuati;
- **Formare e sensibilizzare il personale** sui rischi informatici e sulle corrette pratiche di sicurezza, in modo continuativo e aggiornato;
- **Implementare controlli di accesso** basati sul principio del minimo privilegio e su meccanismi di autenticazione forte;
- **Effettuare verifiche e audit periodici** per valutare l'efficacia delle misure adottate e individuare aree di miglioramento.

L'obiettivo è garantire un livello di protezione adeguato e in costante evoluzione, capace di fronteggiare minacce informatiche sempre più sofisticate e di tutelare in modo efficace dati, sistemi e processi aziendali.

5.2
INCIDENT RESPONSE E BUSINESS CONTINUITY

Ogni fornitore deve disporre di un **piano strutturato di risposta agli incidenti di sicurezza informatica**, che includa procedure chiare e formalizzate per:

In particolare, i fornitori devono:

- **Identificazione tempestiva** di minacce, anomalie e potenziali incidenti attraverso sistemi di monitoraggio, rilevamento e segnalazione;
- **Classificazione e valutazione** dell'incidente in base a gravità, impatto e urgenza, con criteri prestabiliti;
- **Contenimento immediato** per limitare la diffusione dell'attacco e ridurre i danni ai sistemi e ai dati;
- **Risoluzione tecnica e ripristino** dei sistemi compromessi, assicurando la piena operatività delle infrastrutture e applicazioni coinvolte;
- **Comunicazione interna ed esterna**, inclusa la notifica al committente entro tempi definiti e, se richiesto, alle autorità competenti;
- **Analisi post-incident** per identificare le cause radice, definire azioni correttive e prevenire il ripetersi di eventi simili.

In aggiunta, ogni fornitore deve predisporre e mantenere un **Piano di Continuità Operativa (BCP)** e un **Piano di Disaster Recovery (DRP)** per garantire l'erogazione dei servizi anche in caso di eventi critici (ad es. guasti infrastrutturali, attacchi ransomware, disastri naturali).

6. Qualità, innovazione e professionalità

6.0
QUALITÀ, INNOVAZIONE E PROFESSIONALITÀ

I fornitori sono pienamente responsabili della **qualità dei prodotti e dei servizi** che mettono a disposizione di Applied. Ciò implica l'adozione di standard elevati lungo l'intero ciclo di vita delle forniture, con particolare attenzione a:

- **Precisione tecnica e affidabilità:** i prodotti e i servizi devono essere conformi alle specifiche tecniche, ai requisiti normativi e contrattuali, e garantire prestazioni costanti e verificabili.
- **Processi di controllo qualità:** i fornitori devono implementare sistemi strutturati di controllo e monitoraggio, includendo test, verifiche e audit periodici, così da assicurare la conformità ai livelli di servizio concordati.
- **Tracciabilità e documentazione:** ogni fornitura deve essere accompagnata da documentazione completa, trasparente e accurata (manuali, certificazioni, report di prova, schede tecniche), utile a dimostrare la conformità del prodotto/servizio.
- **Professionalità del personale:** il personale coinvolto deve possedere competenze adeguate, aggiornate e certificate, oltre a mantenere standard elevati di etica professionale e responsabilità.

Applied incoraggia inoltre i fornitori a promuovere innovazione tecnologica e metodologica, purché sviluppata e adottata nel rispetto di principi di:

- **Etica e responsabilità:** le innovazioni devono garantire sicurezza, trasparenza e rispetto delle normative vigenti.
- **Sostenibilità:** ogni nuovo processo, metodologia o tecnologia deve essere valutato in termini di impatto ambientale e sociale, favorendo soluzioni a basso impatto e orientate all'efficienza energetica.
- **Sicurezza:** l'adozione di nuove tecnologie deve sempre prevedere un'analisi dei rischi e l'introduzione di adeguate misure di protezione per utenti, dati e infrastrutture.

7. Sostenibilità ambientale e responsabilità sociale

7.0
SOSTENIBILITÀ AMBIENTALE E RESPONSABILITÀ SOCIALE

I fornitori devono contribuire alla riduzione dell'impatto ambientale delle proprie attività attraverso:

- riduzione dei consumi energetici e idrici;
- gestione responsabile dei rifiuti e corretto smaltimento dei RAEE;
- utilizzo di fonti di energia rinnovabile;
- promozione di modelli di lavoro a basso impatto (es. smart working, riunioni da remoto).

Devono inoltre sostenere iniziative sociali e comunitarie, promuovendo comportamenti etici lungo tutta la catena di fornitura

8. Etica nell'Intelligenza artificiale e nell'uso degli algoritmi

8.0
ETICA NELL'INTELLIGENZA ARTIFICIALE E NELL'USO DEGLI ALGORITMI

Nel caso in cui sviluppino o utilizzino sistemi di AI, i fornitori devono garantire:

- **Trasparenza** degli algoritmi, che devono essere documentati e spiegabili;
- **Affidabilità e monitoraggio costante** delle soluzioni;
- **Responsabilità umana** nelle decisioni critiche;
- **Equità** e prevenzione di discriminazioni;
- **Sicurezza** degli algoritmi contro abusi o attacchi.

9. Segnalazioni e Whistleblowing

9.0
SEGNALAZIONI E WHISTLEBLOWING

Applied ha istituito un canale di whistleblowing accessibile anche ai fornitori, che consente di segnalare violazioni o comportamenti illeciti. Il canale è presente sul sito corporate **www.applied.it** .

Le segnalazioni vengono trattate in modo confidenziale, garantendo la protezione dell'identità del segnalante e la tutela da ritorsioni.

I fornitori sono tenuti a collaborare nelle verifiche e ad attuare eventuali azioni correttive.

10. Monitoraggio, audit e conseguenze

10.0
MONITORAGGIO, AUDIT E CONSEGUENZE

Applied si riserva il diritto di verificare la conformità al Codice attraverso audit, ispezioni e richieste di documentazione.

In caso di violazioni:

- potranno essere richieste azioni correttive immediate;
- potrà essere sospesa la collaborazione fino al ripristino della conformità;
- nei casi più gravi o reiterati, il contratto potrà essere risolto.

11. Impegno vincolante del fornitore

11.0
IMPEGNO VINCOLANTE DEL FORNITORE

Con la sottoscrizione del contratto o l'avvio dell'attività, il fornitore dichiara formalmente di:

- aver letto, compreso e accettato il presente Codice di Condotta;
- impegnarsi a rispettarlo in ogni sua parte;
- diffonderne i contenuti all'interno della propria organizzazione e della catena di fornitura;
- collaborare attivamente con Applied in caso di verifiche o richieste di azioni correttive;
- segnalare tempestivamente eventuali violazioni.

12. Aggiornamenti e diffusione

12.0
AGGIORNAMENTI E DIFFUSIONE

Il presente Codice è soggetto a revisioni periodiche, in linea con l'evoluzione normativa, tecnologica e con le esigenze aziendali.

Le versioni aggiornate saranno comunicate a tutti i fornitori e pubblicate sul sito corporate di Applied, affinché siano sempre accessibili e consultabili.

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	Italiano
Approvatore	Head of Staff
Autore	Cyber Security & Compliance Manager
Data di approvazione	01/10/2025
Data classification	Pubblico


applied®
innovation makers