applied®

Codice Etico

6. Cyber security e sicurezza informatica

6.1 PRINCIPI DI SICUREZZA INFORMATICA
6.2 CONFORMITÀ ALLA NORMATIVA (GDPR, NIS2 E ALTRE DIRETTIVE)
6.3 INCIDENT RESPONSE
6.4 PROTEZIONE DEI DATI IN CLOUD
6.5 CYBER RESILIENCE
6.6 RESPONSABILITÀ DEI DIPENDENTI IN MATERIA DI SICUREZZA
6.7 FORMAZIONE CONTINUA

7. Innovazione, professionalità e sostenibilità

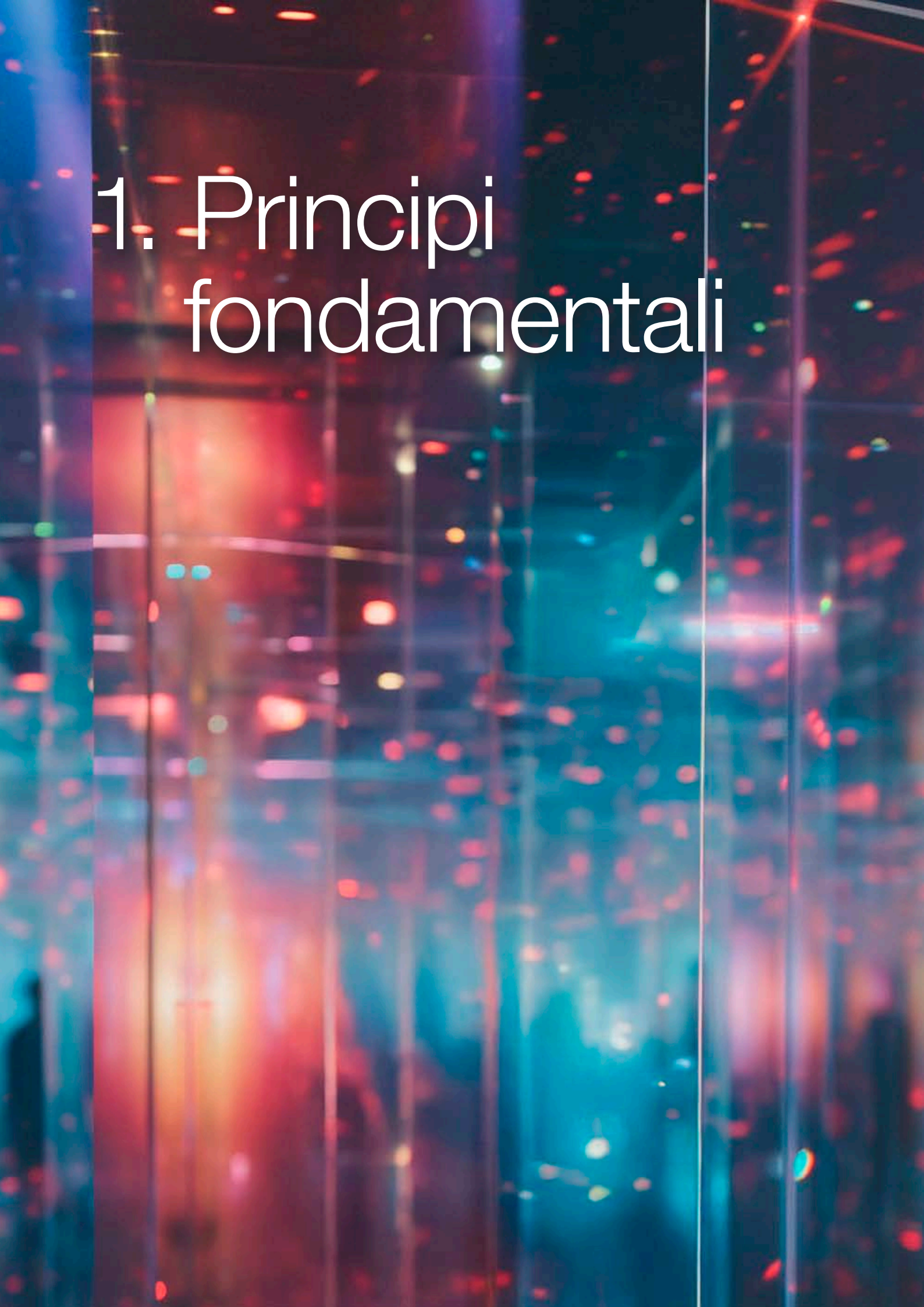
7.1 IMPEGNO PROFESSIONALE
7.2 INNOVAZIONE TECNOLOGICA
7.3 RESPONSABILITÀ AMBIENTALE E SOCIALE

8. Conformità legale e segnalazioni

8.1 RISPETTO DELLE LEGGI
8.2 CANALI DI SEGNALAZIONE

9. Etica nell'intelligenza artificale ed uso degli algoritmi

9.1 PRINCIPI DI AI RESPONSABILE
9.2 GESTIONE ETICA DEI DATI
9.3 IMPATTO SOCIALE E DIRITTI FONDAMENTALI



1. Principi fondamentali

1.1 MISSIONE E VISIONE

Applied nasce con l'obiettivo di offrire soluzioni digitali innovative, sicure e personalizzate, capaci di sostenere la crescita dei propri clienti e di generare valore per l'intera collettività. La nostra visione è quella di costruire un ecosistema tecnologico affidabile, in cui la protezione dei dati, il rispetto delle persone e la sostenibilità rappresentino i principi fondamentali che orientano ogni decisione, azione e strategia aziendale.

Il presente Codice Etico traduce questi valori in norme di comportamento concrete, che definiscono il nostro modo di operare e rafforzano la relazione di fiducia che intendiamo instaurare con i dipendenti, i clienti, i collaboratori, i partner e le comunità. Esso costituisce un riferimento essenziale per garantire integrità, responsabilità e trasparenza in tutte le attività di Applied.

1.2 PRINCIPI GUIDA

I principi su cui fondiamo la nostra identità sono:

- **Integrità**: agire sempre con onestà, trasparenza e coerenza, sapendo che ogni scelta riflette chi siamo con la volontà di costruire una relazione di fiducia con chi ci affida i propri progetti.
- **Responsabilità**: operare con serietà, rigore e consapevolezza, contribuendo al benessere dell'azienda e della comunità.
- **Rispetto**: valorizzare ogni persona nella sua unicità, promuovendo un ambiente di lavoro aperto, inclusivo e collaborativo. Il rispetto ci guida nel creare relazioni basate sull'ascolto, sull'empatia e sulla dignità reciproca.
- **Sicurezza**: proteggere con cura le informazioni, i dati e i sistemi informatici che ci vengono affidati. La sicurezza è un atto di tutela verso clienti, collaboratori e partner, ed è parte integrante del nostro impegno per un ambiente digitale affidabile.
- **Innovazione**: investire nella crescita e sperimentare nuove soluzioni tecnologiche con l'obiettivo di migliorare continuamente, mettendo competenze e creatività al servizio delle persone e dei loro obiettivi.
- **Sostenibilità**: lavorare con responsabilità verso l'ambiente e la società, riducendo gli impatti e supportando un futuro sostenibile, nel quale il progresso convive con il rispetto per le risorse e le comunità.

1.3 PERCHÈ UN CODICE ETICO?

In Applied crediamo che l'etica non sia solo un insieme di regole, ma il fondamento su cui costruire ogni nostra scelta. Il Codice Etico nasce come guida concreta per orientare i comportamenti di tutte le persone che fanno parte della nostra organizzazione o che, a vario titolo, collaborano con essa.

Attraverso il Codice, Applied esprime la propria identità e il proprio impegno nel diffondere una cultura basata su integrità, trasparenza e responsabilità, nel pieno rispetto delle leggi e delle migliori pratiche nazionali e internazionali.

Il Codice rappresenta un patto di coerenza e credibilità: rispettarlo significa tutelare non solo l'organizzazione, ma anche le persone che la compongono e la reputazione che insieme costruiamo.

Essere parte di Applied significa condividere la convinzione che nessun obiettivo economico, vantaggio personale o interesse immediato possa mai giustificare comportamenti contrari ai principi di correttezza e responsabilità che definiscono il nostro modo di operare.

2. Attuazione del codice

2.1
DIFFUSIONE E APPLICAZIONE

Il presente Codice Etico è vincolante per tutti i dipendenti, collaboratori, partner e fornitori che intrattengono rapporti con l'azienda.

Il documento è reso pubblicamente disponibile sul sito corporate di Applied e sulla intranet aziendale, così da permettere a chiunque di consultarne i contenuti e comprenderne i principi.

Ogni soggetto che opera in relazione con la società è tenuto a rispettare e applicare le disposizioni del Codice, integrandole nel proprio comportamento professionale quotidiano.

2.2
AGGIORNAMENTO

Il Codice Etico è soggetto a revisioni periodiche per garantirne la continua coerenza con l'evoluzione normativa, tecnologica e con le esigenze dell'azienda.

Eventuali modifiche o integrazioni vengono approvate dalla Direzione e pubblicate sul sito corporate, così da assicurarne la piena trasparenza e la massima accessibilità per tutti gli stakeholder.

3. Il valore delle persone

3.1
DISCRIMINAZIONE

Applied promuove un ambiente di lavoro basato sul rispetto, sull'equità e sull'inclusione, impegnandosi a prevenire qualsiasi forma di discriminazione o comportamento lesivo della dignità personale. L'azienda vieta ogni forma di disparità di trattamento legata all'età, al genere, all'identità o all'orientamento sessuale, all'origine etnica, alla nazionalità, alla religione, alle opinioni politiche, alla disabilità, allo stato di salute o all'appartenenza sindacale, garantendo pari opportunità di accesso, crescita e sviluppo professionale in tutte le fasi del rapporto di lavoro.

Applied si impegna inoltre a mantenere un ambiente professionale libero da molestie, abusi e comportamenti offensivi di qualsiasi natura. Ogni ruolo di responsabilità deve essere esercitato con imparzialità, rispetto e senso etico, evitando favoritismi o trattamenti ingiustificati. A ciò si affianca l'adozione di procedure di selezione e assunzione trasparenti, fondate esclusivamente su competenze, merito e coerenza con i valori aziendali.

Il rispetto di questi principi costituisce per Applied un presupposto essenziale per costruire una cultura aziendale inclusiva e sostenibile, capace di riconoscere e valorizzare la diversità come risorsa strategica.

3.2
PARITÀ DI GENERE

Applied riconosce la parità di genere come un principio fondamentale di equità e come un valore strategico per la crescita dell'organizzazione. L'azienda promuove un ambiente di lavoro in cui ogni persona possa esprimere pienamente le proprie competenze e aspirazioni, operando in condizioni di uguaglianza e di rispetto reciproco. A tal fine garantisce pari opportunità di accesso, di carriera e di sviluppo professionale, indipendentemente dal genere, assicurando anche un trattamento retributivo equo e coerente con le competenze, le responsabilità e i risultati raggiunti.

Applied adotta processi di selezione, valutazione e promozione trasparenti, basati esclusivamente su criteri di merito e competenza, e sostiene la conciliazione tra vita professionale e personale attraverso soluzioni organizzative inclusive e flessibili.

La parità di genere rappresenta per Applied un elemento imprescindibile per costruire una cultura aziendale fondata sul rispetto, sull'inclusione e sulla valorizzazione delle persone.

3.3
SALUTE E SICUREZZA SUL LAVORO

Applied considera la salute e la sicurezza delle persone una priorità assoluta e un valore essenziale per la sostenibilità delle proprie attività. L'azienda si impegna a garantire un ambiente di lavoro sicuro, salubre e rispettoso della dignità individuale, assicurando in ogni contesto il pieno rispetto delle normative vigenti in materia di tutela della salute e sicurezza.

Applied promuove una cultura della prevenzione, orientata alla consapevolezza dei rischi e all'adozione di comportamenti responsabili da parte di dipendenti e collaboratori.

Ogni lavoratore è tenuto a osservare scrupolosamente le regole aziendali e tutte le misure di sicurezza previste, contribuendo attivamente alla creazione di un ambiente lavorativo protetto. Applied considera infatti la sicurezza una responsabilità condivisa, che richiede l'impegno congiunto dell'organizzazione e delle persone che vi operano per assicurare condizioni di lavoro sicure e sostenibili.

3.4
DIRITTO DI ORGANIZZAZIONE

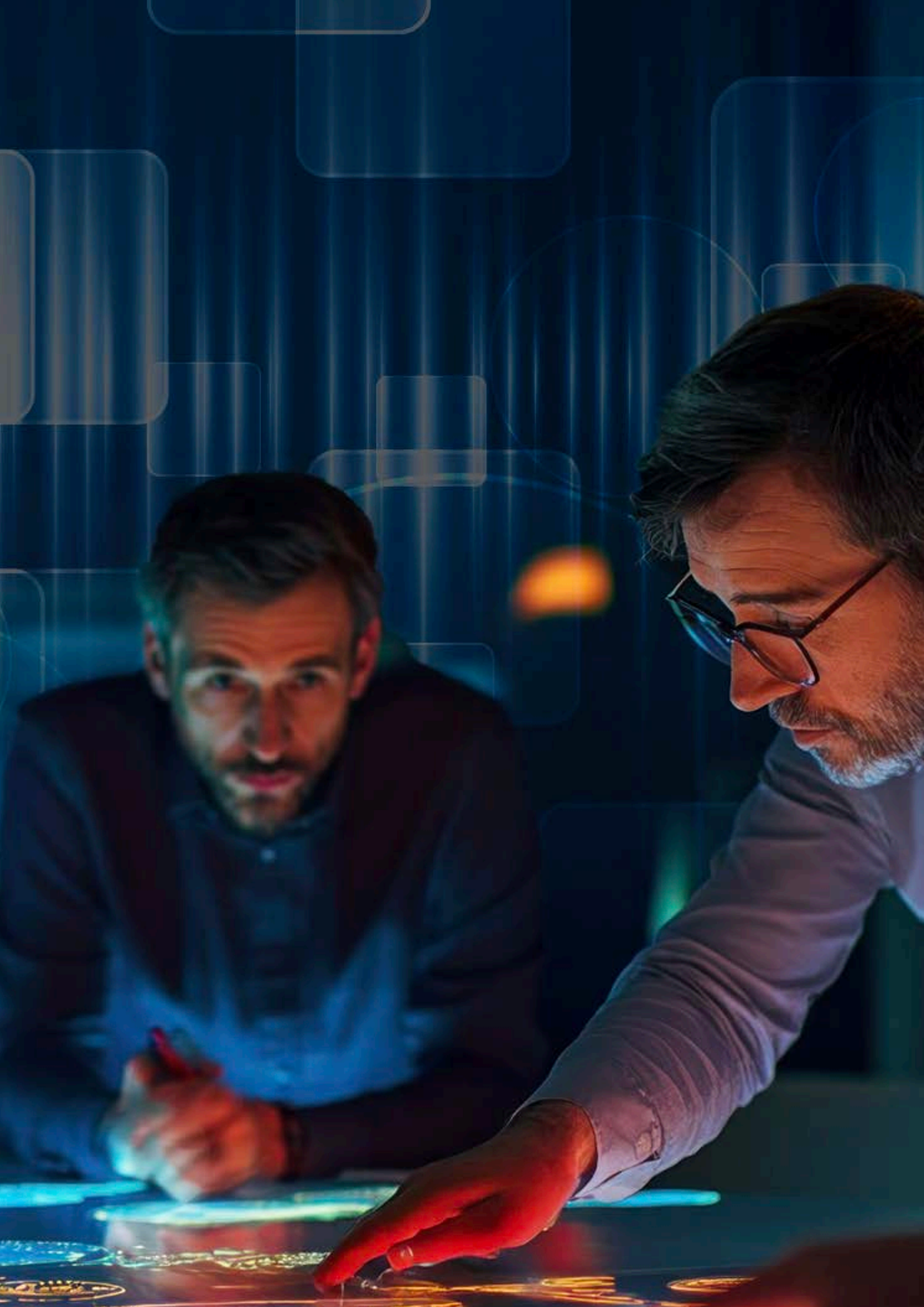
Applied riconosce e tutela il diritto dei lavoratori alla libertà sindacale, nel pieno rispetto delle convenzioni internazionali e delle normative nazionali vigenti. L'azienda garantisce a ogni persona la possibilità di aderire, o di non aderire, a organizzazioni sindacali di propria scelta, senza alcuna forma di discriminazione.

3.5
FORMAZIONE E SVILUPPO DELLE COMPETENZE

Applied considera la formazione continua e lo sviluppo delle competenze come elementi strategici per la crescita professionale delle persone e per il successo sostenibile dell'organizzazione. A tal fine promuove percorsi formativi destinati a sviluppare ogni individuo e ad ampliare sia le competenze tecniche sia quelle trasversali. Applied investe in programmi di aggiornamento e sviluppo professionale in linea con l'evoluzione delle tecnologie, dei mercati e dei processi aziendali, favorendo al contempo una cultura basata sulla conoscenza e sulla collaborazione, nella quale l'apprendimento sia condiviso e accessibile a tutti i livelli dell'organizzazione.

L'azienda incoraggia inoltre la responsabilità individuale nella propria crescita professionale, sostenendo anche iniziative di formazione autogestite o caratterizzate da approcci innovativi. Garantisce pari opportunità di accesso alle attività formative, promuovendo principi di merito, trasparenza e inclusione. Applied ritiene che lo sviluppo delle persone rappresenti un fattore determinante di competitività e innovazione e investe costantemente per valorizzare il capitale umano quale risorsa distintiva dell'impresa.

4. Integrità negli affari



4.1
CONFLITTO DI INTERESSI

I conflitti di interesse si manifestano quando gli interessi personali di un dipendente entrano in contrasto, reale o potenziale, con gli interessi di Applied. Tutte le decisioni, le valutazioni e le attività svolte nell'ambito aziendale devono essere guidate da obiettività, imparzialità e senso di responsabilità professionale.

Ogni situazione che possa generare un conflitto di interesse deve essere tempestivamente segnalata, al fine di prevenire rischi e garantire un ambiente di lavoro trasparente e affidabile. Nel caso in cui un dipendente si trovi, anche solo potenzialmente, in una situazione di conflitto rispetto agli interessi di Applied, egli è tenuto a informarne immediatamente il proprio superiore diretto, che provvederà a valutarne l'impatto e a definire le azioni appropriate.

4.2
LOTTA ALLA CORRUZIONE

Applied condanna ogni forma di corruzione e vieta qualsiasi pratica che possa favorire atti corruttivi nei rapporti professionali, commerciali o istituzionali. È proibito a chiunque operi per conto dell'azienda offrire o accettare denaro, vantaggi o benefici di qualunque natura per influenzare decisioni, ottenere contratti o conseguire indebiti vantaggi competitivi.

Sono consentiti esclusivamente omaggi occasionali di valore modesto e coerenti con le consuetudini locali, purché non possano influenzare, nemmeno potenzialmente, l'esito di relazioni o transazioni commerciali. Ogni dono che non rispetti tali requisiti deve essere rifiutato. È infine vietato porre in essere, direttamente o tramite terzi, comportamenti volti a influenzare impropriamente istituzioni o autorità governative, o a ottenere trattamenti di favore nello svolgimento delle attività aziendali.

4.3
CONCORRENZA LEALE

Applied riconosce che il principio della libera concorrenza costituisce un elemento essenziale per lo sviluppo di un ambiente economico dinamico, a beneficio non solo dei consumatori, ma anche delle imprese. L'attività di innovazione deve essere condotta nel pieno rispetto dei diritti di proprietà intellettuale tutelati dalle norme vigenti.

Al fine di garantire che Applied operi sempre nel quadro della concorrenza libera e leale, è fatto espresso divieto di porre in essere scambi di informazioni riservate, intese o accordi che possano, anche indirettamente, alterare il corretto funzionamento del mercato o compromettere la parità competitiva tra operatori economici.

4.4
FRODE E RICICLAGGIO

Applied basa ogni propria attività su principi di onestà, integrità e correttezza, opponendosi fermamente a qualsiasi forma di illecito o comportamento fraudolento. È vietata qualsiasi operazione, in Italia o all'estero, che possa esporre l'azienda al rischio di ricettazione, riciclaggio o coinvolgimento con organizzazioni criminali.

Nell'avvio di relazioni commerciali, Applied richiede verifiche accurate sulla reputazione e sull'affidabilità delle controparti, così da prevenire ogni possibile violazione delle normative nazionali e internazionali in materia di antiriciclaggio. Il sistema amministrativo, contabile e fiscale deve garantire la massima trasparenza e affidabilità: tutte le operazioni devono essere registrate in modo completo, accurato e veritiero, nel pieno rispetto dei processi decisionali e autorizzativi aziendali.

5. Riservatezza, GDPR e protezione dei dati


applied

5.1 PRINCIPI DI PROTEZIONE DEI DATI (GDPR)

La società garantisce il pieno rispetto del Regolamento (UE) 2016/679 – GDPR e delle normative nazionali in materia di protezione dei dati personali, assicurando che ogni trattamento avvenga nel quadro dei principi fondamentali stabiliti dalla legge. Ogni attività di raccolta ed elaborazione dei dati deve essere svolta nel rispetto dei criteri di liceità, correttezza e trasparenza, garantendo che gli interessati siano sempre adeguatamente informati e che il trattamento sia giustificato da basi legali chiare.

I dati personali vengono trattati esclusivamente per finalità specifiche, esplicite e legittime, evitando qualunque utilizzo incompatibile con gli scopi per i quali sono stati originariamente raccolti. L'azienda applica il principio di minimizzazione, limitando la raccolta e la conservazione alle sole informazioni strettamente necessarie e assicurando che tali dati siano sempre accurati, aggiornati e corretti.

La conservazione dei dati è limitata al tempo strettamente necessario al raggiungimento delle finalità dichiarate, nel rispetto delle disposizioni normative e delle policy interne. La società adotta inoltre misure tecniche e organizzative adeguate a garantire l'integrità e la riservatezza delle informazioni, proteggendole da accessi non autorizzati, perdite accidentali, divulgazioni improprie o distruzioni.

5.2 GESTIONE ETICA DEI DATI

La società si impegna a trattare i dati in modo responsabile ed etico, tenendo conto non solo degli obblighi di legge, ma anche delle implicazioni sociali e morali derivanti dall'utilizzo delle informazioni. È vietato qualsiasi impiego dei dati che possa comportare forme di sfruttamento, discriminazione o violazione dei diritti umani. Nell'ambito dei progetti che prevedono l'utilizzo di tecnologie avanzate, quali intelligenza artificiale, machine learning o analisi di big data, la società adotta un approccio fondato sui principi dell'etica dell'AI, assicurando che gli algoritmi non generino bias o trattamenti discriminatori nei confronti di individui o gruppi sociali. Ogni nuova tecnologia o iniziativa basata sull'analisi dei dati è sottoposta a una valutazione di impatto etico, oltre che legale, al fine di garantire un utilizzo equo, trasparente e conforme ai valori aziendali.

5.3
OBBLIGHI DEI COLLABORATORI

Tutti i collaboratori sono tenuti a rispettare le policy interne in materia di protezione dei dati e tutela della privacy. È vietata la divulgazione, anche se involontaria, di informazioni riservate o di dati personali relativi a clienti, partner o colleghi. Nel caso in cui si verifichi, o si sospetti, una violazione della sicurezza dei dati, il dipendente ha l'obbligo di informare tempestivamente i referenti aziendali competenti, così da consentire l'adozione immediata delle misure necessarie alla gestione dell'incidente.

5.4
SICUREZZA INFORMATICA E ACCESSO AI DATI

Applied adotta misure di cyber security adeguate e proporzionate, che includono sistemi di crittografia, procedure di autenticazione multifattore e controlli di accesso basati su profili autorizzativi. L'accesso ai dati è consentito esclusivamente al personale autorizzato e deve essere sempre tracciato, nel rispetto del principio del least privilege, che limita i permessi al minimo necessario per lo svolgimento delle attività. Le informazioni aziendali e i dati dei clienti non devono essere conservati su supporti non sicuri né condivisi senza adeguate misure di protezione, al fine di prevenire violazioni, dispersioni o utilizzi impropri.

5.5
DIRITTI DEGLI INTERESSATI

Ogni persona i cui dati vengono trattati ha diritto di accesso, rettifica, cancellazione, limitazione, portabilità e opposizione, in conformità alle normative vigenti in materia di protezione dei dati personali. L'azienda si impegna a garantire risposte tempestive, trasparenti e complete a tutte le richieste presentate dagli interessati, assicurando il pieno rispetto dei loro diritti e una gestione responsabile delle informazioni.

6. Cyber security e sicurezza informatica

6.1
PRINCIPI DI SICUREZZA INFORMATICA

La società riconosce la sicurezza delle informazioni come un pilastro fondamentale della propria responsabilità verso le persone e la comunità con cui opera. Proteggere i dati di dipendenti, fornitori, clienti e di tutti gli stakeholder non rappresenta soltanto un obbligo normativo, ma un impegno etico profondo, che riflette la volontà dell'azienda di costruire relazioni basate sulla fiducia, sulla trasparenza e sul rispetto.

Per questo motivo la società ha adottato un Sistema di Gestione della Sicurezza delle Informazioni (ISMS) conforme allo standard internazionale ISO/IEC 27001, che assicura un approccio strutturato, documentato e certificato nella valutazione e nel trattamento dei rischi informatici. Tale sistema consente di proteggere in modo proattivo il patrimonio informativo aziendale e di garantire continuità operativa anche nelle situazioni più critiche.

L'azione dell'azienda si fonda su tre principi guida che rappresentano l'essenza stessa della sicurezza informatica:

- **Riservatezza**, affinché l'accesso ai dati sia sempre limitato alle sole persone autorizzate.
- **Integrità**, per garantire che le informazioni rimangano accurate, complete e non siano soggette a modifiche non autorizzate.
- **Disponibilità**, per assicurare che i servizi e le informazioni necessarie siano fruibili quando richiesto, anche in caso di imprevisti o incidenti.

6.2 CONFORMITÀ ALLA NORMATIVA (GDPR, NIS2 E ALTRE DIRETTIVE)

La società opera nel pieno rispetto del GDPR, della normativa nazionale e della Direttiva (UE) 2022/2555 – NIS2, che introduce requisiti avanzati in materia di cybersecurity per i fornitori di servizi essenziali e digitali. In conformità a tale Direttiva, l'azienda ha adottato misure tecniche e organizzative proporzionate ai rischi, includendo sistemi di monitoraggio continuo, procedure di autenticazione forte e l'impiego di tecniche di crittografia per proteggere i dati e le infrastrutture. La società ha inoltre implementato un sistema strutturato di risk management volto a identificare, prevenire e mitigare le minacce informatiche, insieme a procedure di segnalazione degli incidenti di sicurezza che prevedono l'obbligo di notifica alle autorità competenti entro i tempi stabiliti dalla legge. Particolare attenzione è riservata anche alla gestione della supply chain, attraverso politiche che garantiscono che fornitori e partner rispettino standard di sicurezza adeguati e coerenti con quelli adottati internamente.

L'azienda si impegna a mantenere un costante aggiornamento in materia di compliance, sostenuto da verifiche interne e audit periodici, affinché i livelli di sicurezza e protezione rimangano sempre elevati e conformi all'evoluzione normativa e tecnologica.

6.3 INCIDENT RESPONSE

La società dispone di un Piano di Incident Response che definisce in modo chiaro le responsabilità, i tempi di intervento e le azioni correttive da attuare in caso di attacco informatico o violazione dei dati, garantendo una gestione tempestiva ed efficace degli eventi critici. Inoltre, l'azienda svolge periodici test di resilienza per verificare l'efficacia delle misure di difesa adottate e assicurare un costante miglioramento della propria capacità di prevenzione e risposta agli incidenti di sicurezza.

6.4 PROTEZIONE DEI DATI IN CLOUD

Tutti i servizi cloud utilizzati dall'azienda vengono selezionati sulla base di rigorosi criteri di conformità normativa e della presenza di adeguate certificazioni di sicurezza, tra cui ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018 e CSA STAR. I dati conservati o trattati in ambiente cloud sono protetti attraverso sistemi di crittografia end-to-end, controlli di accesso granulari e strumenti di monitoraggio delle anomalie, al fine di garantire elevati standard di sicurezza e protezione delle informazioni.

6.5 CYBER RESILIENCE

La società promuove la resilienza informatica come capacità essenziale per resistere, assorbire e riprendersi con rapidità ed efficacia da eventuali incidenti cyber. A tal fine adotta sistemi di monitoraggio proattivo che consentono di rilevare e mitigare tempestivamente le minacce, garantendo una protezione continua e sempre aggiornata delle infrastrutture digitali.

I collaboratori sono coinvolti in programmi di formazione continua dedicati alla cyber hygiene, alla prevenzione del phishing e alle tecniche di social engineering, affinché ciascuno possa contribuire in modo consapevole alla sicurezza complessiva dell'organizzazione. Parallelamente, l'azienda mantiene un processo dinamico di valutazione dei rischi emergenti — come ransomware evoluti, attacchi alla supply chain o minacce basate su intelligenza artificiale — così da anticipare scenari critici e rafforzare costantemente le proprie difese.

6.6 RESPONSABILITÀ DEI DIPENDENTI IN MATERIA DI SICUREZZA

L'azienda richiede che tutti i collaboratori utilizzino esclusivamente software autorizzati e conformi alle policy interne, evitando l'installazione di programmi non consentiti o potenzialmente rischiosi. Gli strumenti aziendali devono essere impiegati unicamente per finalità professionali, nel rispetto delle procedure e delle linee guida in materia di sicurezza informatica. Ogni persona è tenuta a segnalare tempestivamente eventuali incidenti di sicurezza, tentativi di phishing o comportamenti sospetti, contribuendo così alla prevenzione delle minacce e alla protezione del patrimonio informativo. I dispositivi aziendali — come computer, laptop e smartphone — devono essere adeguatamente protetti mediante password robuste, sistemi di cifratura e tutte le misure previste per garantirne la sicurezza.

6.7 FORMAZIONE CONTINUA

Tutti i dipendenti partecipano regolarmente a corsi di formazione dedicati al GDPR e alla Cyber Security, così da mantenere un livello elevato di consapevolezza e aggiornamento rispetto alle normative vigenti e alle migliori pratiche in materia di protezione dei dati. La cultura della sicurezza informatica è considerata un elemento fondamentale dell'identità aziendale e si traduce in comportamenti responsabili e attenti da parte di ogni persona. Per rafforzare ulteriormente questa consapevolezza, l'azienda realizza periodiche campagne interne di simulazione di phishing, utili a testare e migliorare la capacità di riconoscere e gestire tentativi di attacco informatico. A queste attività si affianca un flusso costante di comunicazioni formative e informative tramite e-mail dedicate, che forniscono aggiornamenti, consigli pratici e indicazioni operative per un utilizzo sicuro degli strumenti digitali.

7. Innovazione, professionalità e sostenibilità

7.1
IMPEGNO PROFESSIONALE

Ogni servizio rivolto al cliente è realizzato con la massima attenzione alla precisione tecnica, alla sicurezza e all'affidabilità, garantendo standard qualitativi elevati e soluzioni realmente efficaci. I progetti vengono sviluppati considerando le esigenze specifiche di ciascun cliente, attraverso interventi personalizzati e orientati al raggiungimento dei risultati attesi.

Ogni collaboratore è direttamente responsabile della qualità del proprio lavoro e contribuisce in modo attivo al miglioramento continuo dei processi interni, consapevole che l'eccellenza del servizio nasce dall'impegno quotidiano e dalla cura con cui vengono svolte tutte le attività.

7.2
INNOVAZIONE TECNOLOGICA

L'azienda promuove e sostiene l'aggiornamento costante delle competenze dei propri dipendenti, favorendo percorsi di formazione, workshop dedicati e iniziative di autoformazione che incoraggiano la crescita professionale continua. Allo stesso tempo, incentiva lo sviluppo e l'adozione di nuove tecnologie, assicurandosi che ogni innovazione sia introdotta nel rispetto dei principi di eticità, sicurezza e sostenibilità.

Per Applied, innovare non significa soltanto introdurre strumenti tecnologici avanzati, ma anche ricercare modalità di lavoro più efficienti, collaborative e rispettose delle persone. L'innovazione è quindi concepita come un processo culturale e organizzativo, capace di generare valore attraverso il miglioramento continuo e la responsabilizzazione di tutti i collaboratori.

7.3
RESPONSABILITÀ AMBIENTALE E SOCIALE

La società è consapevole che anche il settore informatico genera un impatto sull'ambiente e, per questo, promuove pratiche di eco-efficienza orientate al risparmio energetico, alla riduzione degli sprechi e al corretto smaltimento dei rifiuti elettronici (RAEE). L'azienda adotta e incoraggia modalità di lavoro a minore impatto ambientale, favorendo lo smart working, le riunioni da remoto e l'ottimizzazione degli spostamenti, con l'obiettivo di contribuire a un uso più responsabile delle risorse e alla sostenibilità complessiva delle proprie attività.

8. Conformità legale e segnalazioni

8.1 RISPETTO DELLE LEGGI

Tutte le attività della società devono essere svolte nel pieno rispetto delle leggi nazionali, comunitarie e internazionali applicabili, garantendo un comportamento conforme alle normative in ogni fase dell'operatività aziendale. È rigorosamente vietata qualsiasi azione o pratica che possa risultare illecita, scorretta o contraria alla normativa vigente, anche quando tale comportamento sembri offrire un vantaggio, diretto o indiretto, per l'azienda.

Ogni collaboratore è responsabile delle proprie azioni ed è tenuto a mantenere un comportamento improntato ai principi di legalità, correttezza e trasparenza, contribuendo così alla tutela dell'integrità e della reputazione dell'organizzazione.

8.2 CANALI DI SEGNALAZIONE

La società ha istituito un sistema di whistleblowing che permette a dipendenti, collaboratori, partner e soggetti esterni di segnalare eventuali violazioni del presente Codice Etico, delle normative vigenti o delle procedure aziendali interne. Le segnalazioni possono riguardare comportamenti illegali, non etici o non conformi alle regole dell'organizzazione, e rappresentano uno strumento fondamentale per garantire trasparenza, legalità e integrità nelle attività aziendali.

Tutte le comunicazioni ricevute vengono gestite con la massima riservatezza, tutelando l'identità del segnalante e assicurando che nessuno possa subire ritorsioni o trattamenti discriminatori a seguito della propria segnalazione. Sul sito corporate di Applied è disponibile una sezione dedicata al whistleblowing, contenente il canale ufficiale per l'invio delle segnalazioni e la procedura operativa da seguire.

La gestione delle segnalazioni avviene secondo criteri di imparzialità, tempestività e tracciabilità, garantendo un'analisi accurata dei fatti esposti e l'adozione delle eventuali misure correttive necessarie.

9. Etica nell'intelligenza artificale ed uso degli algoritmi

9.1 PRINCIPI DI AI RESPONSABILE

La società riconosce che l’impiego dell’intelligenza artificiale e degli algoritmi di analisi dei dati offre straordinarie opportunità di innovazione, ma comporta al tempo stesso significative responsabilità etiche e sociali. Per questo motivo si impegna a garantire che tutte le soluzioni basate su IA siano conformi ai requisiti previsti dal Regolamento Europeo sull’Intelligenza Artificiale (AI Act), adottando un approccio rigoroso, trasparente e orientato alla tutela delle persone.

Ogni progetto che prevede l’utilizzo di sistemi di IA deve essere sviluppato nel rispetto di alcuni principi fondamentali. La trasparenza rappresenta un requisito essenziale: gli algoritmi devono essere spiegabili, adeguatamente documentati e comprensibili per gli utenti e gli stakeholder coinvolti. Parimenti importante è l’affidabilità, assicurata attraverso test approfonditi, monitoraggio costante e attività di manutenzione volte a ridurre bias, errori e vulnerabilità. L’azienda afferma con chiarezza il principio della responsabilità umana: ogni applicazione di IA deve avere un referente identificabile che garantisca il corretto utilizzo della tecnologia e mantenga il controllo decisionale (“human in the loop”). L’equità costituisce un ulteriore pilastro, poiché l’IA non deve generare né amplificare discriminazioni basate su genere, etnia, religione, orientamento sessuale, disabilità o caratteristiche personali. Infine, la sicurezza deve essere garantita in ogni fase del ciclo di vita della tecnologia, minimizzando i rischi di manipolazioni, usi impropri o attacchi informatici.

9.2
GESTIONE ETICA DEI DATI

La gestione etica dei dati rappresenta un principio fondamentale dell'operato aziendale. Tutti i dati utilizzati, siano essi impiegati per l'addestramento degli algoritmi o per il loro funzionamento, devono essere raccolti e trattati nel pieno rispetto del GDPR e delle normative vigenti in materia di protezione delle informazioni personali. L'azienda applica rigorose procedure di anonimizzazione, minimizzazione e sicurezza dei dataset, garantendo che le informazioni siano utilizzate esclusivamente quando strettamente necessario e sempre in condizioni adeguate di protezione.

L'organizzazione rifiuta in modo assoluto l'utilizzo di dati provenienti da fonti illecite o da trattamenti che possano ledere i diritti fondamentali delle persone, riconoscendo che la qualità, la liceità e la correttezza dei dati costituiscono un presupposto essenziale per un uso responsabile delle tecnologie digitali. Ogni dataset è sottoposto a una valutazione sistematica di qualità ed eticità, finalizzata a prevenire rischi di bias, distorsioni o discriminazioni, assicurando così che l'impiego dei dati sia sempre coerente con i valori aziendali e con il rispetto della dignità umana.

9.3
IMPATTO SOCIALE E DIRITTI FONDAMENTALI

Le applicazioni di intelligenza artificiale devono essere concepite e utilizzate nel pieno rispetto dei diritti fondamentali della persona, evitando qualunque impiego che possa risultare invasivo o compromettere la dignità e la libertà individuale. L'azienda promuove un uso dell'IA orientato a generare un impatto positivo sulla società, contribuendo al miglioramento dei processi, all'aumento dell'efficienza e alla maggiore accessibilità dei servizi, affinché l'innovazione tecnologica sia sempre al servizio delle persone e del bene comune.

Società di riferimento	**APPLIED**
Perimetro di validità	Aziende gruppo Applied
Ambito documento	COMPLIANCE
Codificazione	APPL-COMPL-PL-001
Nome esteso documento	APPL-COMPL-PL-001-Codice Etico-v01
Documento	Codice Etico
Versione	1 del 24/11/2025
Lingua	Italiano
Approvatore	Head of Staff
Autore	Cyber Security & Compliance Manager
Data di approvazione	24/11/2025
Data classification	Pubblico


applied®
innovation makers