PARTE GENERALE

1. PREMESSA

Il presente Modello di Organizzazione, Gestione e Controllo (di seguito "Modello") è adottato da ATHLOS S.r.l. ai sensi del D.Lgs. 8 giugno 2001 n. 231, che ha introdotto nell'ordinamento italiano la responsabilità amministrativa degli enti per specifiche fattispecie di reato commesse, nel loro interesse o a loro vantaggio, da soggetti in posizione apicale o da soggetti sottoposti alla loro direzione o vigilanza.

Il Decreto ha segnato un'evoluzione significativa del sistema di responsabilità degli enti, richiedendo alle organizzazioni l'adozione di assetti organizzativi e di controllo idonei a prevenire la commissione dei reati presupposto. In tale contesto, il Modello costituisce uno strumento di presidio del rischio penale d'impresa e un elemento strutturale del sistema di governance aziendale.

ATHLOS è una PMI innovativa operante nel settore delle tecnologie digitali avanzate, con particolare riferimento a:

- sviluppo di soluzioni basate su Intelligenza Artificiale e machine learning;
- progettazione e realizzazione di software personalizzato;
- erogazione di servizi digitali in modalità Software as a Service (SaaS) e su infrastrutture cloud;
- progettazione e implementazione di sistemi per Smart Cities, digitalizzazione e automazione;
- realizzazione di piattaforme di data analytics, integrazione dati e soluzioni ad alto contenuto tecnologico.

La natura altamente tecnologica delle attività svolte, l'interazione con sistemi informatici complessi, la gestione di dati – anche potenzialmente sensibili – e la partecipazione a progetti pubblici o partenariati tecnologici rendono necessario un sistema strutturato di prevenzione dei rischi, coerente con il quadro normativo vigente.

L'adozione del Modello non rappresenta un mero adempimento formale, bensì una scelta di governance consapevole e strategica, finalizzata a:

- prevenire la commissione dei reati presupposto previsti dal D.Lgs. 231/2001;

- rafforzare il sistema di controllo interno e la gestione dei rischi;
- assicurare tracciabilità, coerenza e trasparenza nei processi decisionali;
- tutelare l'affidabilità tecnologica, la reputazione e la credibilità dell'azienda nei confronti di clienti, partner e istituzioni;
- promuovere e diffondere una cultura organizzativa improntata alla legalità, all'integrità e alla responsabilità.

Il Modello si inserisce in un sistema più ampio di regole, procedure e presidi organizzativi che concorrono a garantire il corretto svolgimento delle attività aziendali, nel rispetto della normativa applicabile e dei principi etici cui ATHLOS ispira il proprio operato.

2. IL D.LGS. 231/2001

Il D.Lgs. 231/2001 prevede la responsabilità amministrativa dell'ente per determinati reati commessi, nell'interesse o a vantaggio dello stesso, da:

- soggetti che rivestono funzioni di rappresentanza, amministrazione o direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale (c.d. soggetti apicali);
- soggetti sottoposti alla direzione o alla vigilanza di uno dei soggetti apicali.

La responsabilità dell'ente non sostituisce quella della persona fisica che ha materialmente commesso il reato, ma si affianca ad essa, configurando un sistema di responsabilità autonomo e diretto in capo alla società.

Ai fini dell'imputazione della responsabilità è necessario che il reato sia stato commesso nell'interesse dell'ente – ossia con la finalità di favorirlo – oppure a suo vantaggio, quando l'ente abbia tratto un beneficio concreto, anche di natura non esclusivamente economica.

Il Decreto prevede un articolato sistema sanzionatorio che può comprendere:

- sanzioni pecuniarie, determinate secondo un sistema per quote;
- sanzioni interdittive, quali l'interdizione dall'esercizio dell'attività, la sospensione o revoca di autorizzazioni, licenze o concessioni, il divieto di contrattare con la Pubblica Amministrazione, l'esclusione da agevolazioni o contributi;

- la confisca del prezzo o del profitto del reato;
- la pubblicazione della sentenza di condanna.

Le sanzioni interdittive, in particolare, possono incidere in modo significativo sulla continuità aziendale, soprattutto per realtà che operano in settori tecnologici e in ambito pubblico.

L'ente può tuttavia andare esente da responsabilità qualora dimostri di aver adottato ed efficacemente attuato, prima della commissione del fatto, un Modello di Organizzazione, Gestione e Controllo idoneo a prevenire reati della specie di quello verificatosi, e di aver affidato a un Organismo di Vigilanza dotato di autonomi poteri di iniziativa e controllo il compito di vigilare sul funzionamento e sull'osservanza del Modello.

L'effettiva attuazione del Modello, la sua adeguatezza rispetto alla struttura organizzativa e la concreta operatività dei controlli costituiscono, pertanto, elementi centrali ai fini dell'esimente prevista dalla normativa.

3. FINALITÀ DEL MODELLO

Il Modello di Organizzazione, Gestione e Controllo adottato da ATHLOS persegue una pluralità di finalità tra loro integrate, volte a costruire un sistema strutturato di prevenzione del rischio-reato coerente con la natura e la complessità delle attività aziendali.

In particolare, il Modello è finalizzato a:

1. **Individuare le attività sensibili**

Identificare e mappare le aree aziendali e i processi nel cui ambito possono essere astrattamente commessi reati rilevanti ai sensi del D.Lgs. 231/2001, tenendo conto della specificità del settore tecnologico in cui opera ATHLOS (sviluppo software, soluzioni AI, servizi SaaS, partecipazione a gare pubbliche, gestione dati e infrastrutture cloud).
Tale attività di analisi consente di concentrare l'attenzione sui processi maggiormente esposti a rischio e di calibrare i presidi di controllo in modo proporzionato.

2. **Definire protocolli decisionali e operativi**

Prevedere protocolli e procedure idonei a regolamentare la formazione e l'attuazione delle decisioni aziendali nelle aree sensibili, assicurando tracciabilità, segregazione delle funzioni, autorizzazioni

formalizzate e controlli preventivi e successivi.
I protocolli costituiscono strumenti concreti di prevenzione, in quanto disciplinano in modo chiaro "chi fa cosa", con quali limiti e secondo quali modalità.

3. **Regolare la gestione delle risorse finanziarie**

Individuare modalità di gestione e controllo delle risorse finanziarie idonee a prevenire la commissione di reati, attraverso principi di trasparenza, tracciabilità dei flussi economici, separazione dei poteri autorizzativi e controlli contabili coerenti con le dimensioni aziendali.
Particolare attenzione è riservata alla gestione di pagamenti, incassi, contributi pubblici, rendicontazioni e rapporti economici con fornitori e partner.

4. **Introdurre obblighi informativi verso l'Organismo di Vigilanza**

Definire flussi informativi strutturati verso l'Organismo di Vigilanza, sia periodici sia su evento, al fine di consentire un'efficace attività di monitoraggio sull'attuazione del Modello e sull'emersione di eventuali criticità.
La trasparenza nei confronti dell'OdV costituisce elemento essenziale per garantire la concreta efficacia del sistema di controllo.

5. **Prevedere un sistema disciplinare adeguato ed efficace**

Introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello e nel Codice Etico, in modo proporzionato alla gravità della violazione e coerente con la normativa applicabile.
L'effettività del sistema sanzionatorio rappresenta condizione imprescindibile ai fini dell'idoneità del Modello.

6. **Promuovere formazione e consapevolezza interna**

Assicurare adeguati percorsi di informazione e formazione rivolti ai destinatari del Modello, con particolare attenzione ai ruoli maggiormente esposti a rischio, al fine di diffondere la conoscenza della normativa 231, delle regole interne e delle responsabilità individuali.
La prevenzione dei reati si fonda, infatti, non solo su regole formali, ma anche sulla consapevolezza e sulla cultura della legalità diffusa all'interno dell'organizzazione.

Nel loro insieme, tali finalità concorrono a costruire un sistema di prevenzione organico, dinamico e coerente con l'evoluzione tecnologica e organizzativa di ATHLOS, orientato al miglioramento continuo e alla tutela dell'integrità aziendale.

4. ASSETTO SOCIETARIO E GOVERNANCE

ATHLOS è amministrata da un Amministratore Unico, cui è attribuita la responsabilità della gestione complessiva della società, nel rispetto delle disposizioni di legge e statutarie.

All'Amministratore Unico competono, in particolare:

- la gestione ordinaria e straordinaria dell'impresa;
- la rappresentanza legale della società nei confronti dei terzi e delle autorità;
- l'adozione, l'approvazione e l'aggiornamento del Modello di Organizzazione, Gestione e Controllo ai sensi del D.Lgs. 231/2001;
- la nomina dell'Organismo di Vigilanza, nonché la definizione delle modalità di funzionamento dello stesso;
- la supervisione sull'efficace attuazione del sistema di controllo interno e sulla coerenza dell'assetto organizzativo rispetto ai rischi aziendali.

L'Amministratore Unico assicura che il Modello sia concretamente attuato e non rimanga un mero documento formale, garantendo l'assegnazione di adeguate risorse finanziarie, organizzative e professionali necessarie al suo funzionamento, nonché promuovendo una cultura aziendale improntata alla legalità, all'integrità e alla responsabilità.

5. ORGANISMO DI VIGILANZA (ODV)

Ai sensi dell'art. 6 del D.Lgs. 231/2001, ATHLOS ha istituito un Organismo di Vigilanza in composizione monocratica, dotato dei requisiti di legge e delle caratteristiche necessarie a garantire l'effettività del sistema di controllo previsto dal Modello.

L'Organismo di Vigilanza opera in piena:

- autonomia e indipendenza, senza vincoli gerarchici o funzionali rispetto alla struttura operativa, con accesso diretto alle informazioni rilevanti;
- professionalità, possedendo competenze adeguate in materia giuridica, organizzativa e di controllo interno, nonché conoscenza del settore tecnologico in cui opera la società;

- continuità d'azione, assicurando un monitoraggio costante e sistematico sull'attuazione e sull'aggiornamento del Modello.

Tali requisiti garantiscono che l'Organismo di Vigilanza possa svolgere in modo efficace e imparziale le proprie funzioni di controllo, prevenzione e proposta di miglioramento del sistema 231 adottato da ATHLOS.

5.1 Funzioni dell'OdV

L'Organismo di Vigilanza svolge un ruolo centrale nel sistema di prevenzione dei rischi ai sensi del D.Lgs. 231/2001 ed è investito delle seguenti funzioni:

- vigilare sull'efficacia e sull'adeguatezza del Modello, verificando che lo stesso sia idoneo a prevenire i reati rilevanti e coerente con l'evoluzione dell'organizzazione e delle attività aziendali;
- monitorare l'osservanza del Codice Etico e delle procedure interne, accertando il rispetto delle regole e dei protocolli previsti;
- ricevere, esaminare e gestire le segnalazioni relative a presunte violazioni del Modello o del Codice Etico, assicurando riservatezza, imparzialità e tracciabilità delle verifiche svolte;
- formulare proposte di aggiornamento o adeguamento del Modello, in relazione a modifiche normative, organizzative o a criticità emerse;
- effettuare verifiche e audit mirati, anche su specifici processi sensibili, avvalendosi – ove necessario – del supporto di funzioni interne o consulenti esterni qualificati.

Attraverso tali attività, l'OdV contribuisce in modo continuativo al mantenimento dell'efficacia e della dinamicità del sistema di controllo adottato da ATHLOS.

5.2 Flussi informativi

Al fine di consentire all'Organismo di Vigilanza un efficace esercizio delle proprie funzioni di controllo e monitoraggio, devono essere tempestivamente trasmesse all'OdV tutte le informazioni rilevanti ai fini del D.Lgs. 231/2001, con particolare riferimento a eventi, situazioni o circostanze che possano incidere sull'adeguatezza e sull'efficacia del Modello.

In particolare, rientrano tra le informazioni oggetto di flusso informativo obbligatorio:

- la partecipazione a procedure di gara pubblica, nonché eventuali affidamenti, aggiudicazioni o esclusioni;
- la costituzione o la partecipazione a Raggruppamenti Temporanei di Imprese (RTI) o ad altre forme di partenariato per progetti pubblici;
- l'avvio o la gestione di contenziosi con la Pubblica Amministrazione o con soggetti pubblici;
- incidenti di sicurezza informatica che possano avere rilevanza sotto il profilo dei reati informatici o del trattamento illecito di dati;
- eventi di data breach o violazioni dei dati personali, anche qualora già oggetto di comunicazione alle autorità competenti;
- anomalie contabili o irregolarità nella gestione dei flussi finanziari;
- segnalazioni ricevute attraverso i canali di whistleblowing;
- rilievi, ispezioni, richieste o contestazioni formulate da autorità di vigilanza o organismi di controllo.

Tali flussi informativi devono essere garantiti con modalità strutturate, documentate e tempestive, al fine di consentire all'OdV di valutare eventuali criticità e proporre, ove necessario, interventi correttivi o aggiornamenti del Modello.

6. STRUTTURA ORGANIZZATIVA E RUOLI ICT

ATHLOS si avvale di una struttura tecnica interna altamente qualificata, organizzata in modo coerente con la natura tecnologica e innovativa delle attività svolte.

In particolare, l'organizzazione comprende:

- un CTO / Responsabile tecnico, con funzioni di indirizzo strategico e supervisione delle attività di sviluppo e innovazione tecnologica;
- un Responsabile IT e infrastrutture, incaricato della gestione delle architetture tecnologiche, degli ambienti cloud e della sicurezza operativa dei sistemi;
- sviluppatori software e specialisti AI, dedicati alla progettazione, implementazione e manutenzione delle soluzioni digitali;

- un team di progettazione e delivery, responsabile dell'analisi dei requisiti, della gestione dei progetti e dell'erogazione dei servizi ai clienti;
- personale dedicato alla gestione e monitoraggio dei servizi SaaS, inclusa la manutenzione applicativa, il supporto tecnico e la continuità operativa.

La presenza di tali ruoli interni consente ad ATHLOS di presidiare in modo diretto e strutturato i processi tecnologici, garantendo tracciabilità, controllo e responsabilizzazione delle attività rilevanti anche ai fini del D.Lgs. 231/2001.

6.1 Rilevanza ICT ai fini 231

In considerazione della natura altamente tecnologica delle attività svolte da ATHLOS, i processi IT e di sviluppo software assumono particolare rilevanza ai fini della prevenzione dei rischi previsti dal D.Lgs. 231/2001.

Le attività connesse alla progettazione, sviluppo, gestione ed erogazione di soluzioni digitali – incluse quelle in modalità SaaS e su infrastrutture cloud – possono infatti esporre l'organizzazione a specifici profili di rischio, tra cui:

- reati informatici;
- trattamento illecito di dati personali o riservati;
- accessi abusivi a sistemi informatici o telematici;
- alterazione, manipolazione o distruzione di dati;
- vulnerabilità nella sicurezza degli ambienti cloud;
- violazioni della normativa in materia di proprietà intellettuale e tutela del software.

Al fine di presidiare tali rischi, ATHLOS adotta un insieme strutturato di principi e misure organizzative e tecniche, tra cui:

- segregazione delle funzioni, con chiara distinzione tra ruoli di sviluppo, test, rilascio e gestione operativa;
- controllo degli accessi, basato su criteri di autorizzazione, profilazione e principio del "least privilege";

- logging e monitoraggio delle attività, al fine di garantire tracciabilità e rilevazione di eventuali anomalie;
- processi formalizzati di change management, per la gestione controllata delle modifiche ai sistemi e alle applicazioni;
- gestione documentata dei rilasci software, con versionamento, validazione e approvazione delle release;
- adozione di un Secure Development Lifecycle (SDLC), volto a integrare requisiti di sicurezza fin dalle fasi di analisi, progettazione, sviluppo, test e manutenzione del software.

Tali presidi concorrono a garantire l'integrità, la riservatezza e la disponibilità delle informazioni trattate, nonché la conformità delle attività tecnologiche ai principi di legalità e controllo previsti dal Modello.

7. UTILIZZO DI CLOUD PROVIDER

In considerazione della natura altamente tecnologica delle attività svolte da ATHLOS, i processi IT, di sviluppo software e di gestione delle infrastrutture digitali rivestono un ruolo centrale nell'ambito del sistema di prevenzione dei rischi previsto dal D.Lgs. 231/2001.

L'azienda progetta, sviluppa ed eroga soluzioni digitali avanzate, anche in modalità SaaS e su infrastrutture cloud, gestendo architetture complesse, ambienti di sviluppo e produzione, basi dati e flussi informativi integrati. Tale contesto operativo può esporre l'organizzazione a specifici profili di rischio rilevanti ai fini 231, tra cui:

- commissione di reati informatici, quali accesso abusivo a sistemi informatici o telematici, detenzione e diffusione illecita di credenziali, danneggiamento di informazioni o sistemi;
- trattamento illecito di dati personali o informazioni riservate, anche in violazione della normativa privacy;
- accessi non autorizzati a sistemi aziendali o di clienti;
- alterazione, manipolazione o distruzione di dati, anche a seguito di errori, carenze procedurali o condotte dolose;

- vulnerabilità o carenze nei presidi di sicurezza degli ambienti cloud utilizzati per l'erogazione dei servizi;
- violazioni della normativa in materia di diritto d'autore e tutela della proprietà intellettuale, incluse eventuali irregolarità nell'utilizzo di software di terze parti o componenti open source.

Al fine di presidiare in modo adeguato tali rischi, ATHLOS adotta un sistema integrato di misure organizzative, procedurali e tecniche, ispirato ai principi di prevenzione, tracciabilità e responsabilizzazione.

In particolare, sono implementati:

- principi di segregazione delle funzioni, con distinzione tra attività di sviluppo, test, validazione, rilascio e gestione operativa, al fine di evitare concentrazioni indebite di poteri;
- controlli sugli accessi logici, basati su criteri di autorizzazione preventiva, profilazione coerente con il ruolo e applicazione del principio del "least privilege";
- sistemi di logging e monitoraggio, volti a garantire la tracciabilità delle attività svolte sui sistemi e la tempestiva rilevazione di anomalie o comportamenti anomali;
- procedure formalizzate di change management, che disciplinano l'introduzione di modifiche a sistemi, applicazioni e infrastrutture, con valutazione preventiva dell'impatto e approvazione documentata;
- processi strutturati di rilascio software, comprensivi di versionamento, validazione tecnica, collaudo e approvazione prima della messa in produzione;
- l'adozione di un Secure Development Lifecycle (SDLC), che integra requisiti di sicurezza fin dalle fasi di analisi dei requisiti, progettazione, sviluppo, test e manutenzione evolutiva, riducendo il rischio di vulnerabilità applicative.

Tali presidi concorrono a garantire l'integrità, la riservatezza e la disponibilità delle informazioni trattate, nonché la conformità delle attività tecnologiche ai principi di legalità, correttezza e controllo previsti dal presente Modello.

7.1 Presidi di controllo

In relazione ai fornitori di servizi cloud e infrastrutturali, considerati soggetti critici ai fini della continuità operativa, della sicurezza delle informazioni e della conformità normativa, ATHLOS adotta specifici presidi di controllo volti a garantire affidabilità, trasparenza e adeguatezza dei servizi erogati.

In particolare, sono previste:

- procedure di selezione basate su criteri oggettivi e documentabili, che tengano conto di competenza tecnica, solidità, certificazioni di sicurezza e reputazione del provider;
- verifica preventiva dei requisiti di sicurezza e protezione dei dati, inclusa la valutazione delle misure tecniche e organizzative adottate dal fornitore;
- formalizzazione contrattuale con clausole specifiche di compliance, comprensive di obblighi in materia di D.Lgs. 231/2001, protezione dei dati personali (GDPR), sicurezza delle informazioni e continuità del servizio;
- monitoraggio periodico dei livelli di servizio (SLA) e delle performance contrattuali;
- attività di audit documentale o verifiche di conformità, ove previste contrattualmente o ritenute necessarie in base al livello di rischio;
- gestione segregata degli ambienti di sviluppo, test e produzione (dev/test/prod), al fine di prevenire interferenze non autorizzate e ridurre il rischio di alterazione o compromissione dei dati.

Tali misure consentono ad ATHLOS di mantenere un adeguato livello di controllo anche sulle attività esternalizzate, assicurando che l'utilizzo di infrastrutture cloud sia coerente con i principi di sicurezza, legalità e prevenzione dei rischi previsti dal Modello.

8. PARTECIPAZIONE A GARE PUBBLICHE E RTI

ATHLOS opera anche nell'ambito dei contratti pubblici e dei progetti complessi, partecipando a procedure di affidamento e iniziative collaborative attraverso diverse modalità organizzative e contrattuali.

In particolare, la società:

- partecipa direttamente a gare pubbliche, presentando offerte in qualità di operatore economico singolo per l'affidamento di servizi e soluzioni tecnologiche;

- prende parte a Raggruppamenti Temporanei di Imprese (RTI), assumendo il ruolo di mandataria o mandante, nell'ambito di progetti che richiedono competenze integrate e multidisciplinari;
- aderisce a partenariati tecnologici e collaborazioni strategiche, finalizzati alla realizzazione di progetti innovativi, alla partecipazione a bandi complessi o allo sviluppo congiunto di soluzioni digitali avanzate.

Tali modalità operative, pur rappresentando opportunità di crescita e innovazione, comportano specifici profili di rischio in relazione ai rapporti con la Pubblica Amministrazione, alla gestione delle dichiarazioni e della documentazione di gara, nonché alla corretta regolamentazione dei rapporti tra partner.

Per tale ragione, la partecipazione a gare, RTI e partenariati è disciplinata da protocolli interni volti a garantire trasparenza, tracciabilità, correttezza e piena conformità alla normativa applicabile e ai principi del presente Modello.

8.1 Rischi specifici

In relazione alla partecipazione a gare pubbliche, alla gestione di contratti con la Pubblica Amministrazione e all'eventuale accesso a contributi o finanziamenti, ATHLOS riconosce l'esistenza di specifici profili di rischio rilevanti ai sensi del D.Lgs. 231/2001.

In particolare, assumono rilievo:

- reati contro la Pubblica Amministrazione, quali corruzione, indebita induzione, abuso d'ufficio o altre condotte idonee a compromettere la correttezza dei rapporti istituzionali;
- turbativa delle procedure di gara, attraverso comportamenti volti ad alterare la libera concorrenza, la parità di trattamento tra operatori o la regolarità della procedura;
- falsità ideologica o materiale in atti e dichiarazioni, incluse eventuali attestazioni non veritiere rese in sede di partecipazione a gare o nella fase esecutiva del contratto;
- indebita percezione di contributi, sovvenzioni o finanziamenti pubblici, anche mediante l'omissione di informazioni rilevanti o la rappresentazione non corretta dei requisiti;
- irregolarità nella rendicontazione delle spese o nell'esecuzione delle prestazioni contrattuali, tali da determinare un vantaggio economico non legittimo o un utilizzo non conforme delle risorse pubbliche.

Tali rischi sono oggetto di specifici presidi organizzativi e procedurali volti a garantire la massima trasparenza, tracciabilità e correttezza nelle interazioni con la Pubblica Amministrazione e nella gestione delle risorse pubbliche.

8.2 Presidi

Al fine di prevenire i rischi connessi alla partecipazione a gare pubbliche e alla gestione di rapporti con la Pubblica Amministrazione, ATHLOS adotta specifici presidi organizzativi e procedurali volti a garantire trasparenza, correttezza e tracciabilità delle attività svolte.

In particolare, sono previsti:

- processi di validazione interna delle offerte, che prevedono verifiche tecniche, economiche e amministrative prima della presentazione, con approvazione formale da parte dei soggetti autorizzati;
- tracciabilità dei contatti e delle interlocuzioni con la Pubblica Amministrazione, attraverso registrazione e conservazione delle comunicazioni rilevanti;
- segregazione dei ruoli nelle fasi di predisposizione, verifica e approvazione dell'offerta, al fine di evitare concentrazioni indebite di poteri e garantire controlli incrociati;
- controllo preventivo e documentato delle dichiarazioni rese, con verifica della veridicità e completezza delle informazioni trasmesse;
- tracciabilità dei flussi finanziari, in particolare con riferimento a pagamenti, incassi, contributi e rendicontazioni, assicurando la coerenza tra attività svolte e corrispettivi percepiti;
- disciplina chiara dei rapporti tra mandataria e mandanti nei Raggruppamenti Temporanei di Imprese (RTI), con definizione delle responsabilità, dei flussi informativi e delle modalità di gestione delle attività e dei corrispettivi.

Tali presidi contribuiscono a garantire la conformità alle disposizioni normative in materia di contratti pubblici e ai principi di legalità e correttezza previsti dal presente Modello.

9. AREE DI RISCHIO RILEVANTI

In considerazione delle attività svolte, della struttura organizzativa e dei rapporti intrattenuti con clienti pubblici e privati, le principali categorie di reato rilevanti ai sensi del D.Lgs. 231/2001 per ATHLOS sono le seguenti.

9.1 Reati contro la Pubblica Amministrazione

Rientrano in tale categoria le fattispecie connesse ai rapporti con enti pubblici, autorità e stazioni appaltanti, tra cui, a titolo esemplificativo:

- corruzione e indebita induzione a dare o promettere utilità;
- traffico di influenze illecite;
- turbativa delle procedure di gara;
- frode nelle pubbliche forniture;
- indebita percezione di contributi o finanziamenti pubblici.

Tali rischi assumono particolare rilievo per ATHLOS in relazione alla partecipazione a gare pubbliche, alla gestione di contratti con la PA e alla rendicontazione di eventuali contributi o progetti finanziati.

9.2 Reati informatici

Considerata la natura tecnologica dell'attività aziendale, risultano rilevanti le fattispecie di reato informatico, tra cui:

- accesso abusivo a sistema informatico o telematico;
- detenzione e diffusione abusiva di codici di accesso;
- danneggiamento di dati, programmi o sistemi informatici;
- intercettazione, impedimento o interruzione illecita di comunicazioni informatiche;
- frodi informatiche.

Tali rischi possono manifestarsi nell'ambito dello sviluppo software, della gestione delle infrastrutture cloud e dei servizi SaaS.

9.3 Trattamento illecito di dati

In relazione alla gestione di dati personali e informazioni riservate, risultano rilevanti:

- trattamento illecito di dati personali;
- comunicazione o diffusione illecita di dati;
- violazioni delle misure di sicurezza previste dalla normativa privacy;
- data breach derivanti da condotte dolose o gravemente colpose.

La gestione di basi dati, piattaforme digitali e sistemi integrati rende tale categoria particolarmente significativa per ATHLOS.

9.4 Reati societari

Rientrano in questa categoria:

- false comunicazioni sociali;
- ostacolo all'esercizio delle funzioni delle autorità di vigilanza;
- irregolarità nella formazione del bilancio o nella gestione contabile;
- indebita restituzione di conferimenti o altre condotte pregiudizievoli per il patrimonio sociale.

Tali fattispecie sono connesse alla gestione amministrativa e finanziaria dell'impresa.

9.5 Corruzione tra privati

Assume rilievo la fattispecie di corruzione tra privati, che può configurarsi nei rapporti commerciali con clienti, partner o fornitori qualora vengano promessi o corrisposti vantaggi indebiti per ottenere trattamenti di favore o condizioni contrattuali privilegiate.

9.6 Riciclaggio e autoriciclaggio

Rientrano tra i rischi:

- riciclaggio di denaro, beni o utilità di provenienza illecita;
- impiego di denaro di provenienza illecita;
- autoriciclaggio.

Tali fattispecie possono essere rilevanti in relazione alla gestione dei flussi finanziari, ai pagamenti verso fornitori e ai rapporti con partner commerciali.

9.7 Violazioni della proprietà intellettuale

Considerata l'attività di sviluppo software e soluzioni tecnologiche, risultano rilevanti:

- violazioni del diritto d'autore;
- utilizzo non autorizzato di software o componenti di terze parti;
- uso non conforme di licenze;
- indebita appropriazione o divulgazione di codice sorgente o know-how.

La tutela della proprietà intellettuale rappresenta un elemento centrale per un'azienda operante nel settore dell'innovazione digitale.

10. PRINCIPI GENERALI DI CONTROLLO

Il sistema di controllo interno adottato da ATHLOS è strutturato in modo da prevenire la commissione dei reati rilevanti ai sensi del D.Lgs. 231/2001 e da garantire correttezza, trasparenza e tracciabilità delle attività aziendali.

Esso si fonda sui seguenti principi generali:

- Separazione delle funzioni, mediante una chiara attribuzione di ruoli e responsabilità, al fine di evitare concentrazioni indebite di poteri e garantire controlli incrociati tra chi propone, chi autorizza, chi esegue e chi verifica;
- Tracciabilità dei processi decisionali, assicurando che ogni decisione rilevante sia documentata, motivata e ricostruibile, con evidenza delle responsabilità coinvolte;
- Autorizzazioni formalizzate e coerenti con il sistema di deleghe, in modo che ogni operazione significativa sia approvata da soggetti muniti dei necessari poteri e nel rispetto dei limiti stabiliti;

- Controllo e trasparenza nella gestione delle risorse finanziarie, attraverso procedure contabili strutturate, tracciabilità dei flussi economici e verifiche periodiche sulla coerenza tra operazioni effettuate e documentazione di supporto;
- Gestione documentale strutturata e sicura, che garantisca conservazione, integrità, accessibilità e protezione delle informazioni rilevanti, nel rispetto delle normative applicabili;
- Monitoraggio continuo dei rischi ICT, con particolare attenzione alla sicurezza dei sistemi informativi, alla protezione dei dati e alla resilienza delle infrastrutture tecnologiche;
- Verifiche e controlli periodici, sia interni sia eventualmente affidati a soggetti terzi, finalizzati a valutare l'efficacia dei presidi adottati e a individuare tempestivamente eventuali criticità.

L'insieme di tali principi assicura un sistema di controllo interno coerente con la complessità organizzativa e tecnologica di ATHLOS, orientato al miglioramento continuo e alla prevenzione dei rischi di natura penale e amministrativa.

11. SISTEMA DI DELEGHE E PROCURE

Il sistema di deleghe e procure adottato da ATHLOS costituisce uno strumento essenziale di presidio organizzativo e di prevenzione dei rischi ai sensi del D.Lgs. 231/2001.

Le deleghe:

- sono formalizzate per iscritto, con data certa e accettazione da parte del delegato;
- definiscono in modo chiaro e puntuale ambito di competenza, poteri attribuiti, limiti operativi e responsabilità connesse;
- risultano coerenti con l'organigramma aziendale e con le effettive funzioni svolte, evitando sovrapposizioni o ambiguità nei ruoli;
- sono oggetto di verifica e aggiornamento periodico, in occasione di modifiche organizzative, variazioni di ruolo o ampliamento delle attività aziendali.

Il sistema di deleghe è strutturato in modo da garantire adeguata segregazione delle funzioni, proporzionalità tra poteri attribuiti e responsabilità assunte, nonché piena tracciabilità delle decisioni rilevanti, contribuendo così all'efficace attuazione del Modello.

12. WHISTLEBLOWING

ATHLOS garantisce un sistema di segnalazione conforme ai principi di riservatezza, tutela e imparzialità, quale strumento fondamentale di prevenzione e controllo nell'ambito del Modello 231.

In particolare, l'azienda assicura:

- la disponibilità di canali di segnalazione riservati e accessibili, idonei a consentire l'invio di comunicazioni relative a presunte violazioni del Modello, del Codice Etico o della normativa applicabile;
- la tutela dell'identità del segnalante, nel rispetto della normativa vigente in materia di whistleblowing e protezione dei dati personali;
- il divieto di qualsiasi forma di ritorsione, discriminazione o penalizzazione nei confronti di chi effettui una segnalazione in buona fede;
- una gestione imparziale, indipendente e documentata delle segnalazioni, affidata ai soggetti competenti, con adeguata istruttoria e tracciabilità delle verifiche svolte.

Il sistema di segnalazione rappresenta uno strumento di garanzia per l'organizzazione e per le persone che vi operano, favorendo l'emersione tempestiva di eventuali criticità e contribuendo al miglioramento continuo del sistema di controllo interno.

13. SISTEMA DISCIPLINARE

La violazione delle disposizioni contenute nel presente Modello costituisce inadempimento agli obblighi contrattuali e può determinare l'applicazione di sanzioni proporzionate alla natura e alla gravità del comportamento accertato.

L'irrogazione delle misure disciplinari avviene nel pieno rispetto:

- del CCNL applicabile;
- della normativa vigente;
- delle disposizioni contrattuali e statutarie;
- dei principi di gradualità e proporzionalità.

Il sistema disciplinare è strutturato in modo differenziato in funzione della qualifica del soggetto coinvolto e del rapporto giuridico con la società. In particolare, sono previste misure specifiche per:

- soggetti apicali, in relazione alle responsabilità di direzione e rappresentanza;
- dipendenti, secondo quanto previsto dal contratto collettivo applicato e dal sistema disciplinare interno;
- collaboratori e consulenti, mediante l'applicazione delle clausole contrattuali previste;
- fornitori, attraverso strumenti contrattuali quali diffida, sospensione o risoluzione del rapporto;
- partner tecnologici, mediante clausole di compliance e, nei casi più gravi, risoluzione del contratto e richiesta di risarcimento danni.

L'effettività del sistema disciplinare costituisce elemento essenziale ai fini dell'idoneità del Modello e della sua concreta attuazione.

14. FORMAZIONE

ATHLOS riconosce la formazione quale elemento essenziale per l'effettiva attuazione del Modello e per la diffusione di una cultura aziendale orientata alla legalità e alla prevenzione dei rischi.

A tal fine, la società assicura:

- percorsi di formazione generale sul D.Lgs. 231/2001, rivolti a tutto il personale, finalizzati a illustrare i principi della responsabilità amministrativa degli enti, i contenuti del Modello e gli obblighi comportamentali previsti;
- formazione specifica per i ruoli ICT, con approfondimenti sui rischi connessi ai reati informatici, alla sicurezza delle informazioni, alla protezione dei dati e alla gestione delle infrastrutture cloud;
- formazione dedicata al personale coinvolto in gare pubbliche e rapporti con la Pubblica Amministrazione, con focus sui reati contro la PA, sulla correttezza delle dichiarazioni e sulla gestione delle procedure di affidamento;
- aggiornamenti periodici, anche in occasione di modifiche normative, evoluzioni organizzative o introduzione di nuovi processi e tecnologie.

Le attività formative sono documentate e calibrate in funzione del livello di esposizione al rischio dei diversi ruoli aziendali, al fine di garantire consapevolezza e responsabilizzazione effettiva dei destinatari del Modello.

15. AGGIORNAMENTO DEL MODELLO

Il Modello è oggetto di aggiornamento periodico e ogniqualvolta intervengano circostanze che possano incidere sulla sua adeguatezza ed efficacia.

In particolare, l'aggiornamento è previsto:

- in caso di modifiche normative o evoluzioni giurisprudenziali rilevanti ai fini del D.Lgs. 231/2001;
- in occasione dell'introduzione di nuovi prodotti o servizi SaaS, di nuove architetture tecnologiche o di significative evoluzioni infrastrutturali (es. nuovi ambienti cloud o modelli di erogazione);
- in caso di ingresso in nuovi mercati, ampliamento delle attività nei confronti della Pubblica Amministrazione o modifiche sostanziali del modello di business;
- su proposta dell'Organismo di Vigilanza, a seguito di verifiche, segnalazioni o criticità emerse;
- in esito al riesame periodico effettuato dall'Amministratore Unico, volto a valutare l'efficacia complessiva del sistema di controllo interno.

L'aggiornamento del Modello costituisce parte integrante del processo di miglioramento continuo e assicura la coerenza del sistema 231 rispetto all'evoluzione organizzativa, tecnologica e normativa di ATHLOS.

16. INTEGRAZIONE CON IL SISTEMA DI CONTROLLO INTERNO

Il Modello 231 è parte integrante del sistema di governance aziendale e si coordina con:

- Codice Etico;
- policy sicurezza informazioni;
- policy data protection;
- policy procurement;
- policy gestione gare;
- procedure amministrative e contabili.