Modello di Organizzazione, Gestione e Controllo preventivo ex D. Lgs. 231/01

ALTINTECH s.r.l.

Viale dell'Umanesimo, 69 Roma (RM)

Documento	***MO01***	*TOT PAGINE: 68*
Revisione	*3.0*	
Emesso il	*01/12/2023*	

	SETTORE	***NOME***	***FIRMA***
Approvato	*Presidente CdA*	*R. Festa*	

File: MO231_e1_r3

SEZIONE I - PARTE GENERALE

0. INTRODUZIONE

0.1 OBIETTIVO DEL DOCUMENTO

Il presente documento è finalizzato a disegnare e formalizzare un **Modello di Organizzazione, Gestione e Controllo preventivo** redatto ai sensi e per gli effetti di cui all'**art. 6 del D. Lgs. n. 231/2001** (pubblicato sulla Gazzetta Ufficiale del 19 giugno 2001 n. 140).

0.2 STRUTTURA DEL DOCUMENTO

Il presente Documento si articola in più sezioni:

- **Parte Generale**, dedicata a:
  - esporre i **principi generali** (normativa di riferimento, linee guida) e l'approccio in base ai quali il Modello è stato costruito;
  - istituire ed illustrare **alcune componenti essenziali del Modello** ed in particolare l'Organismo di Vigilanza, il Codice Etico, le modalità di divulgazione del Modello (Formazione ed informazione), il Sistema Disciplinare;
  - individuare la **mappa generale delle aree aziendali a rischio** in relazione alle fattispecie di reato che si potrebbero manifestare;
- **Parti Speciali** dedicate a:
  - l'analisi delle **singole fattispecie di reato** applicabili in relazione alla specifica attività di **ALTINTECH s.r.l.** e le **regole speciali di condotta a carattere preventivo** specificamente adottate per tipologia di rischio-reato. (A-G)
  - le modalità di **prevenzione del rischio:** i **sistemi generali di controllo**. (H)
  - Procedura del sistema di **controllo di gestione**. (I)

0.3 LEGENDA

Direzione (soci operativi: Presidente, amministratore delegato, Direttore Generale, Direzioni operative) "D"

Consiglio di Amministrazione "CdA"

Modello organizzativo, gestionale e di controllo preventivo di seguito denominato "Modello"

Organismo di Vigilanza di seguito denominato "OdV"

Contratto Collettivo Nazionale di Lavoro Metalmeccanico CONFAPI di seguito denominato "CCNL"

1. NORMATIVA DI RIFERIMENTO

1.1 LA RESPONSABILITÀ AMMINISTRATIVA

Il **D. Lgs. n. 231/2001** relativo alla "Disciplina della responsabilità amministrativa delle persone giuridiche, delle cooperative e delle associazioni anche prive di personalità giuridica" introduce nel nostro ordinamento **la responsabilità amministrativa (in sede penale) delle persone giuridiche** derivante da reati commessi nel loro interesse o a loro vantaggio da parte di soggetti:

- che rivestono **funzioni di rappresentanza**, **di amministrazione o di direzione** dell'azienda o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, nonché di **persone che esercitano, anche di fatto, la gestione o il controllo della stessa;**

- **sottoposti alla direzione o alla vigilanza** di uno dei soggetti sopra indicati.

1.2 I REATI PERSEGUITI

I **reati contemplati dalla normativa** in oggetto e rilevanti per l'azienda, sono i seguenti:

A) REATI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE

I reati previsti dal D. Lgs. 231/01 nei rapporti con la P.A. sono di seguito sintetizzati:

- Malversazione a danno dello Stato e dell'Unione Europea (art. 316-bis c.p)
- Indebita percezione di erogazioni in danno dello Stato o dell'Unione Europea (art. 316-ter c.p.)
- Truffa aggravata in danno dello Stato, di altro ente pubblico o dell'Unione Europea (art. 640, comma 2 n.1, c.p.)
- Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.)
- Frode informatica in danno dello Stato o altro ente pubblico (art. 640-ter c.p.)
- Corruzione per un atto d'ufficio o contrario ai doveri d'ufficio (artt. 318-319-319 bis-320 c.p.)
- Istigazione alla corruzione (art. 322 c.p.)
- Corruzione in atti giudiziari (art. 322 c.p.)
- Traffico di influenze illecite (artt.346-bis C.P. 601 e 602 c.p.).

- DL 14 luglio 2020 n. 75 Attuazione della direttiva (UE) 2017/1371, relativa alla lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale.

B) REATI SOCIETARI

- False comunicazioni sociali (art. 2621 c.c.);
- False comunicazioni sociali in danno dei soci o dei creditori (art. 2622, commi 1 e 3, c.c.);
- Impedito controllo (art. 2625, comma 2, c.c.);
- Indebita restituzione dei conferimenti (art. 2626 c.c.);
- Illegale ripartizione degli utili e delle riserve (art. 2627 c.c.);
- Operazioni in pregiudizio dei creditori (art. 2629 c.c.);
- Formazione fittizia del capitale (art. 2632 c.c.);
- **Corruzione tra privati (estesa dalla L. 190/12 nei casi previsti dall'art. 2635 c.c.);**
- Illecita influenza sull'assemblea (art. 2636 c.c.).

C) REATI INFORMATICI

- Frode informatica; D. Lgs. 184/2021, attuativo della Direttiva 2019/713 (lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti) e modifica del testo del delitto di "Frode informatica", di cui all'art. 640-ter, introducendo una nuova circostanza aggravante nel caso in cui dalla alterazione del sistema informatico derivi un trasferimento "di denaro, di valore monetario o di valuta virtuale".
- Falsità in un documento informatico pubblico o avente efficacia probatoria (Art.491-bis C.P.)
- Accesso abusivo ad un Sistema informatico o telematico (Art. 615-ter C.P.)
- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (Art. 615-quater C.P.)
- Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (Art. 615-quinquies C.P.)

- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (Art. 617-quater)

- Trattamento illecito di dati, falsità nelle dichiarazioni e notificazioni al Garante della privacy, inosservanza delle misure minime di sicurezza e di protezione dei dati personali (artt. 167 - 172 D. Lgs. n.196/2003 – **Regolamento Europeo 16/679**).

- Danneggiamento di informazioni, dati e programmi informatici. (Art. 635-bis)

- Danneggiamento di sistemi informatici o telematici. (Art. 635-quater)

D) REATI COMMESSI IN VIOLAZIONE DELLE NORME ANTINFORTUNISTICHE E SULLA TUTELA DELL'IGIENE E DELLA SALUTE SUL LAVORO

- Omicidio colposo (art. 589 c.p.)

- Lesioni personali colpose (art. 590 ter c.p.)

In considerazione delle attività oggi svolte dalla **ALTINTECH s.r.l.** nonché del documento di valutazione dei rischi predisposto ai sensi del D. Lgs 81/2008 e s.m.i., le attività a rischio per le quali potrebbero ravvisarsi gli estremi per la commissione dei reati in discussione sono limitate e riconducibili:

- allo svolgimento di attività lavorative con utilizzo di archivi e postazioni con videoterminali;

- allo svolgimento di attività lavorative di carattere impiantistico ed edile in cantieri temporanei esterni;

- all'accesso, transito e permanenza nei locali in uso all'azienda;

- all'accesso, transito e permanenza nei locali messi a disposizione da committenti e clienti per lo svolgimento di attività di presidio e manutenzione.

E) RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA, NONCHÉ AUTORICICLAGGIO (art. 25-octies, d. lgs 231/01)

- D. Lgs. 195/2021 Attuazione della Direttiva UE 2018/1673 in materia di lotta al riciclaggio mediante il diritto penale.

F) REATI AMBIENTALI

- Attività di gestione rifiuti non autorizzata. Effettuazione di un'attività di raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione di rifiuti, in mancanza della prescritta autorizzazione, iscrizione o comunicazione. Art.256 c.1 ("Attività di gestione rifiuti non autorizzata") D. Lgs.03.04.2006, n. 152 ("Norme in materia ambientale")

- Attività di gestione di rifiuti non autorizzata. Realizzazione o gestione di una discarica non autorizzata. Art.256 c.3 I periodo ("Attività di gestione rifiuti non autorizzata") D. Lgs.03.04.2006, n.152 ("Norme in materia ambientale")

- Attività di gestione di rifiuti non autorizzata. Fattispecie: Attività non consentite di miscelazione di rifiuti (in violazione dell'art.187 del D. Lgs.03.04.2006, n.152). Art.256 c.5 ("Attività di gestione rifiuti non autorizzata") D. Lgs.03.04.2006, n.152 ("Norme in materia ambientale")

- Mancata effettuazione della bonifica del suolo, del sottosuolo, delle acque superficiali o delle acque sotterranee, dopo averne cagionato l'inquinamento, con superamento delle cd. "concentrazioni soglia di rischio". Art.257 ("Bonifica dei siti") c.1 e 2 D. Lgs.03.04.2006, n.152 ("Norme in materia ambientale").
- Traffico illecito di rifiuti. Art.259 ("Traffico illecito di rifiuti") c.1 D. Lgs.03.04.2006, n. 152 ("Norme in materia ambientale")

- Attività organizzate per il traffico illecito di rifiuti. Cessione, ricevimento, trasporto, esportazione, importazione, gestione abusiva di ingenti quantitativi di rifiuti, al fine di conseguire un ingiusto profitto, con più operazioni e attraverso l'allestimento di mezzi e attività continuative organizzate. Art.260 c.1 e 2 ("Attività organizzata per il traffico illecito di rifiuti") D. Lgs.03.04.2006, n.152 ("Norme in materia ambientale")

- Fornitura-nella predisposizione di un certificato di analisi di rifiuti, utilizzato nell'ambito del sistema di controllo della tracciabilità dei rifiuti -di false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti. Inserimento di un certificato falso nei dati da fornire ai fini della tracciabilità dei rifiuti. Art.260 bis ("Sistema informatico di controllo della tracciabilità rifiuti") c.6 D. Lgs.03.04.2006, n.152 ("Norme in materia ambientale") Art.483 C.P.

- Omissione dell'accompagnamento del trasporto di rifiuti pericolosi con la copia cartacea della Scheda SISTRI-Area Movimentazione e, ove necessario, sulla base della normativa vigente, con la copia del certificato analitico che identifica le caratteristiche dei rifiuti. Art.260 bis ("Sistema informatico di controllo della tracciabilità rifiuti") c.7 II periodo D. Lgs.03.04.2006, n.152 ("Norme in materia ambientale") - Art. 483 C.P.

- Uso di un certificato di analisi di rifiuti contenente false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti, durante il trasporto. Art.260 bis ("Sistema informatico di controllo della tracciabilità rifiuti") c.7 ultimo periodo D. Lgs.03.04.2006, n.152 ("Norme in materia ambientale")

- Art.483 C.P.

G) IMPIEGO DI CITTADINI DI PAESI TERZI IL CUI SOGGIORNO È IRREGOLARE (art. 25-doudecies)

- Testo Unico sull'immigrazione, (D.L. 25 Luglio 1998 n.286 come modificato dal D.L. 23 Maggio 2008 n.92 art. 22, c. 12.
- D.L.vo 16 Luglio 2012 n. 109
- terzo comma dell'art. 603 bis c.p.

1.3 LE SANZIONI

Le **sanzioni** previste a carico della **ALTINTECH s.r.l.** per gli illeciti commessi possono essere di tipo pecuniario e, nei casi più gravi, anche interdittive (interdizione dall'esercizio dell'attività, sospensione o revoca autorizzazioni, ecc.).

1.4 L'ESONERO DALLA RESPONSABILITÀ

Il D. Lgs. n. 231/01 tuttavia consente una forma di **esonero della ALTINTECH s.r.l. dalla responsabilità in oggetto**, se si dimostra, in sede di procedimento penale per uno dei reati previsti dal Decreto, di aver adottato ed attuato con efficacia **modelli di organizzazione gestione e controllo idonei a prevenire la commissione dell'illecito**.

Il **Modello** deve pertanto:

- descrivere gli **strumenti, i protocolli e le precauzioni adottate** dalla **ALTINTECH s.r.l.** per prevenire il compimento dei reati indicati dal Decreto;

- essere applicato in modo tale da non poter essere eluso, se non fraudolentemente; la vigilanza sul suo funzionamento e sulla sua osservanza, nonché il suo aggiornamento, devono essere affidati ad un **apposito organismo** dotato di autonomi poteri di iniziativa e di controllo.

2. MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO

2.1 PRINCIPI GENERALI

Il sistema dei controlli si fonda su alcuni **principi di base** affinché risulti idoneo agli scopi per cui è stato posto in essere:

- deve essere un processo continuo o almeno **svolto con periodicità adeguata**, quindi non una tantum;

- deve ridurre il rischio ad un livello **"accettabile"**.
  La soglia di "accettabilità" è rappresentata da **un sistema di prevenzione non aggirabile se non fraudolentemente o intenzionalmente**: è infatti concepito in modo da evitare che un qualunque soggetto operante all'interno della **ALTINTECH s.r.l.** possa giustificare la propria condotta adducendo l'ignoranza delle direttive aziendali o l'errore - dovuto anche a negligenza o imperizia – nella valutazione delle direttive stesse.

2.1 STRUTTURA DEL MODELLO

Le **componenti del sistema di controllo preventivo**, necessarie affinché risulti idoneo a prevenire il rischio accettabile, sono:

- **codice etico o di comportamento** con riferimento ai reati disciplinati dal D. Lgs. 231/01, sulla cui base impiantare il modello organizzativo;
  - ➔ **approvato contestualmente alla prima edizione del presente documento e verificato, integrato e aggiornato se del caso ad ogni audit annuale**
  - ➔ **integrato da sistema anticorruzione ISO 37001 e dichiarazione**
  - ➔ **integrato da dichiarazione contro la schiavitù**

- **sistema organizzativo formalizzato** e chiaro in relazione soprattutto all'attribuzione di responsabilità alle linee di dipendenza gerarchica, alla descrizione dei compiti, ai principi di controllo;
  - ➔ **sistema di gestione certificato ISO 9001**
  - ➔ **sistema di gestione certificato ISO 14001**
  - ➔ **sistema di gestione certificato ISO 45001**

- **sistemi informativi/procedure aziendali** atti a regolamentare lo svolgimento delle attività prevedendo gli opportuni punti di controllo;
  - ➔ **sistema di gestione certificato ISO 9001;**
  - ➔ **dossier privacy (Regolamento EU 16/679 - GDPR);**
  - ➔ **sistema di gestione certificato ISO 14001;**
  - ➔ **sistema di gestione certificato ISO 45001**
  - ➔ **sistema SA 8000**
  - ➔ **sistema EMAS**
  - ➔ **sistema di procurement sostenibile ISO 20400**

- **sistema di deleghe/poteri autorizzativi e di firma** assegnati in coerenza alle responsabilità organizzative e gestionali;
  ➔ **sistema di gestione certificato ISO 9001**
  ➔ **sistema di gestione certificato ISO 14001**
  ➔ **sistema di gestione certificato ISO 45001**

- **sistemi di controllo di gestione** in grado di fornire tempestiva segnalazione di situazioni di criticità gestionale e finanziario;
  ➔ **controllo amministrativo da parte di consulente esterno**
  ➔ **audit periodici dell'ODV**

- **sistema per le segnalazioni di illeciti e irregolarità cd. "Whistleblowing"** in grado di fornire tempestiva segnalazione di situazioni di che riguardano comportamenti, rischi, reati o irregolarità, consumati o tentati;
  ➔ **audit periodici dell'ODV**
  ➔ **sistema anticorruzione ISO 37001**
  ➔ **procedura ex D.lgs. n. 24/2023**
  ➔ **sistema di gestione certificato ISO/IEC 27001**

- **sistema disciplinare formalizzato** e noto;
  ➔ **riportato nel presente documento da CNL applicato**

- **comunicazione al personale e sua formazione** in relazione alle componenti del sistema di controllo preventivo, caratterizzato da una comunicazione capillare, dettagliata, chiara, reiterata nel tempo.
  ➔ **pianificazione dell'ODV**

Le componenti del sistema di controllo interno devono essere integrate in un **sistema organico** che rispetti i seguenti principi:

- verificabilità, documentabilità, tracciabilità, coerenza e congruità di ogni operazione;
- separazione delle funzioni, per cui nessuno può gestire in autonomia un intero processo;
- trasparenza delle regole e dei criteri;
- documentazione dei controlli.

3. ADOZIONE DEL MODELLO

3.1 MOTIVAZIONI ALL'ADOZIONE DEL MODELLO

Il management della **ALTINTECH s.r.l.,** tramite l'adozione del Modello, intende porre in attuazione protocolli organizzativi volti alla **prevenzione del rischio** di concretizzazione dei reati oggetto del D. Lgs. 231/01e s.m.i. , sensibilizzando sia i dipendenti che i soggetti esterni sulle linee di comportamento che l'impresa si attende e sulla correttezza e trasparenza nella gestione delle proprie attività.

3.2 APPROCCIO PER FASI

Nella redazione del presente Modello, si è proceduto con un approccio per fasi:

1. identificazione dei rischi dello specifico contesto aziendale, ossia **individuazione delle aree in cui possono verificarsi le fattispecie di reato**;

2. strutturazione di **protocolli organizzativi e di comportamento** per la prevenzione del rischio, ossia di un sistema strutturato ed organico di prevenzione, dissuasione e controllo costruito partendo dalla valutazione del sistema oggi esistente all'interno dell'azienda ed adeguandolo affinché risulti idoneo ridurre il rischio di reato ad un livello accettabile.

Fase 1 - Identificazione dei rischi
L'identificazione dei rischi è avvenuta tramite:

A) Individuazione delle aree aziendali a rischio:
In questa fase il management, con il supporto di esperti esterni, ha analizzato l'attività tramite interviste con persone-chiave e con il supporto di documentazione interna (disegno organizzativo, procedure aziendali della qualità, incarichi, gestione informativa) focalizzandosi principalmente su:

- processi o attività che richiedono interfaccia con la Pubblica Amministrazione e con l'esterno in generale;
- processi o attività che possano configurare reati di tipo societario;
- processi o attività che configurino impatti ambientali significativi;
- processi o attività con rischi per la salute e sicurezza dei lavoratori;
- soggetti in possesso di facoltà di individuazione, indicazione e/o direzione delle scelte dell'impresa relativamente ad attività "a rischio di reato" per la loro frequenza, per il tipo di poteri coinvolti, per la natura o rilevanza dell'oggetto o per le risorse economiche impiegate.

B) Analisi dei reati potenziali:
In questa fase è stata effettuata una ricostruzione delle possibili modalità attuative dei reati rispetto al contesto relazionale interno ed esterno in cui opera l'impresa.
In ognuna delle aree a rischio, si è individuato quale tipo di reato può essere commesso, da chi, come e quando, analizzando le procedure, le responsabilità o i poteri di firma, le apposite misure predisposte per evitare che i dipendenti o gli amministratori possano

commettere reati, ecc., con particolare attenzione alla dirigenza ed al ruolo ad esso assegnato nel garantire all'interno dell'impresa il rispetto delle regole e della legge.

C) Indicazione delle misure preventive:
Per ogni tipologia di reato sono stati indicati nel modello protocolli di comportamento e procedure aziendali volti a limitare il rischio di commissione dei reati considerati.

Fase 2 - Adeguamento del sistema organizzativo

A) Analisi del sistema organizzativo "AS IS":
In questa fase è stato analizzato il complessivo sistema organizzativo e le sue componenti per verificarne l'idoneità a prevenire il rischio.
In particolare si è verificata:

- la formalizzazione ed adeguata diffusione dell'organigramma e del mansionario in modo da esplicitare la suddivisione di compiti e delle responsabilità;
- la coerenza del sistema delle deleghe tramite l'individuazione degli organi individuali o collegiali con facoltà deliberative, i soggetti con potere di rappresentanza dell'impresa nei confronti dei terzi, i limiti nei quali questi ne possono utilizzare le risorse economiche, le prassi che presiedono al regolare funzionamento aziendale e rispetto a processi decisionali esterni;
- la presenza di procedure informatiche tali da regolamentare lo svolgimento delle attività e consentire accessi differenziati in funzione della separazione dei compiti;
- un sistema di controllo dell'attività e dei rischi;
- la completezza e coerenza del sistema in ordine ai suoi elementi costitutivi (presenza del Codice Etico, dell'Organismo di Vigilanza, del Sistema disciplinare, di adeguata formazione al personale dipendente, ecc.).

L'analisi è stata effettuata ricorrendo alla documentazione aziendale del sistema Qualità, del sistema di monitoraggio del sistema informativo e della privacy e ad interviste con personale "chiave".

B) Valutazione e adeguamento del sistema:
A seguito dell'analisi del sistema organizzativo e di controllo ad oggi, si è valutata la sua completezza ed adeguatezza a svolgere funzioni di prevenzione del rischio e di indirizzo delle attività del personale operativo e manageriale verso l'efficiente conseguimento degli obiettivi aziendali.

Il sistema organizzativo è stato quindi:

- **adeguato in modo tale da consentire che i rischi di commissione di reati compresi dal D. Lgs. 231/01 siano ridotti ad un livello "accettabile", come sopra definito;**

- **integrato delle componenti ritenute essenziali ove mancanti o parziali.**

3.3 ADOZIONE E GESTIONE DEL MODELLO

Il Modello è stato sottoposto al Consiglio di Amministrazione per l'approvazione dei contenuti e la costituzione dell'Organismo di Vigilanza.

3.4 MODIFICHE E INTEGRAZIONI AL MODELLO

Il presente documento rappresenta un “atto di emanazione dell’organo dirigente”. La sua adozione iniziale e le relative modifiche – fatto salvo quanto di competenza dell’OdV – sono rimesse alla competenza del Consiglio di Amministrazione.

4. ORGANISMO DI VIGILANZA (ODV)

4.1 IDENTIFICAZIONE DELL'ODV

L'Organismo di Vigilanza è una delle componenti essenziali del Modello, come previsto dall'art. 6 D. Lgs. 231/01.

Per rappresentare un efficace strumento di prevenzione e controllo, deve garantire:

- **autonomia ed indipendenza, professionalità e continuità di azione** (requisiti oggettivi);
- **onorabilità ed assenza di conflitti di interessi** o rapporti di parentela con gli organi sociali ed i vertici aziendali da parte dei componenti (requisiti soggettivi).

Nel rispetto dei principi sopra citati, **ALTINTECH s.r.l.** ha affidato l'incarico di OdV a un organo costituito dalla seguente figura professionale:

- **esperto sistemi di controllo di gestione e auditing;**

L'OdV è collocato in staff al Presidente.

4.2 FUNZIONAMENTO DELL'ODV

La composizione, nomina e revoca dell'OdV è attribuzione del CdA.

La revoca dell'OdV può avvenire:

- per giusta causa (negligenza, infedeltà, inefficienza, ecc.);
- per impossibilità sopravvenuta;
- per il venire meno dei requisiti soggettivi di onorabilità, assenza di conflitto di interessi, assenza di parentela con i vertici aziendali o organi sociali;
- per il venire meno dei requisiti oggettivi di imparzialità, autonomia, professionalità, continuità dell'azione o rapporto di dipendenza /collaborazione con **ALTINTECH s.r.l.**;

L'OdV così costituito provvederà a stabilire proprie norme di funzionamento, ed è in ogni caso tenuto a riunirsi in via ordinaria con frequenza minima ogni sei mesi. Delle riunioni dell'OdV dovrà essere tenuto regolare verbale.

4.3 ATTRIBUZIONI E POTERI DELL'ODV

4.3.1 Mission

All'OdV è attribuito il compito di vigilare su:

- **idoneità del modello** a prevenire i reati previsti dal Decreto in relazione alla struttura aziendale;

- **osservanza delle prescrizioni** e dei principi del Modello da parte dei destinatari;

- **aggiornamento del Modello** laddove necessiti di adeguamento per assicurarne l'efficacia.

4.3.2 Attività

Dal punto di vista operativo, le attività di competenza dell'OdV sono:

- **vigilanza e controllo sul rispetto dei principi del Modello e sull'applicazione delle procedure in esso previste.**
  L'attività in oggetto potrà avvenire tramite indagini conoscitive interne, verifiche mirate su atti, operazioni, transazioni con particolare riguardo per le operazioni a rischio, accesso a tutta la documentazione aziendale necessaria, e tramite tutti gli atti ritenuti idonei alle verifiche, nel rispetto della normativa ed informando le funzioni coinvolte. Le verifiche saranno oggetto di apposito reporting ai soggetti destinatari;

- **verifica periodica dell'adeguatezza del Modello** in ordine alla sua reale capacità di prevenire i comportamenti illeciti, tramite ad esempio la revisione periodica delle aree di rischio, la verifica della completezza delle procedure aziendali, l'analisi delle modifiche nei processi, ecc.;

- **adeguamento del Modello** in funzione della naturale evoluzione del contesto aziendale, ad esempio rivedendo la mappa dei rischi;

- **attività propositiva e consultiva su misure di prevenzione del rischio** nei confronti degli organi sociali o delle funzioni aziendali in grado di garantirne l'applicazione, in merito a modifiche / aggiornamento al Modello ove non di diretta competenza dell'OdV, emanazione di direttive aziendali per disciplinare operazioni a rischio, ecc.;

- **coordinamento con altre funzioni aziendali o con gli organi sociali** in modo da consentire una compartecipazione trasversale di tutta l'azienda nel garantire l'efficacia del Modello applicato;

- **monitoraggio della formazione periodica** attivata in azienda relativamente alle materie oggetto del D. Lgs. 231/01 e della chiarezza e trasparenza dell'informazione, ad esempio verificando la diffusione tramite pubblicazione in rete del Modello, concordando il piano di formazione relativo e controllandone l'esecuzione periodica,

monitorando l'adeguata divulgazione di organigramma, funzionigramma, sistema sanzionatorio, ecc.;

- **informazione ed aggiornamento degli organi sociali**(si veda "Attività di reporting dell'OdV verso gli altri organi aziendali").

Si specifica che il ruolo dell'OdV non ha carattere coercitivo per cui le sanzioni o misure disciplinari potranno essere comminate solo dagli organi sociali competenti nel rispetto della normativa vigente e non potrà in modo autonomo modificare la struttura o i processi aziendali.

4.3.3 Salvaguardia

Al fine di **garantire l'autonomia e indipendenza** dei membri dell'OdV da eventuali ritorsioni a loro danno, tutte le decisioni di carattere straordinario relative a membri dell'OdV saranno prese dal CdA.

4.4 ATTIVITÀ DI REPORTING DELL'ODV VERSO GLI ALTRI ORGANI AZIENDALI

L'OdV è tenuto riportare:

- su **base continuativa**, anche verbalmente, al Presidente circa le criticità emerse od ipotesi di reato individuate e sull'attività svolta;

- **almeno annualmente** tramite relazione scritta al CdA indicando:
  - la sintesi delle attività svolte;
  - i controlli effettuati ed il loro esito;
  - gli aspetti di maggior rilevanza emersi;
  - le proposte di adeguamento del Modello, compresa la revisione della mappa delle aree a rischio;
  - il piano delle ispezioni previste per l'anno successivo.

Qualora le ipotesi di reato riguardino uno degli organi sopra citati, l'OdV dovrà riferire tempestivamente a uno degli altri organi.

Il CdA ha facoltà di convocare l'OdV in ogni momento, così come l'OdV per motivi particolarmente gravi ed urgenti potrà richiedere ai soggetti competenti la convocazione dei predetti organi.

Gli incontri tra l'OdV e gli Organi sopra citati dovranno essere oggetto di verbale.

4.5 OBBLIGHI DI INFORMAZIONE NEI CONFRONTI DELL'ODV

4.5.1 Segnalazioni da parte di esponenti aziendali o da parte di terzi e "Whistleblowing"

L'OdV deve essere informato tramite apposite segnalazioni, da parte di tutti i portatori di interesse (esterni ed interni) che hanno rapporti con **ALTINTECH s.r.l.**, in merito a atti o eventi che potrebbero ingenerare responsabilità ai sensi del D. Lgs. 231/01 (cfr. Codice Etico art. 22).

Le segnalazioni per violazioni o presunte violazioni al Modello da parte di:

- un dipendente: dovranno essere effettuate in primis al suo diretto superiore. Qualora le segnalazioni non abbiano esito o il dipendente abbia qualche remora a coinvolgere direttamente il proprio superiore, potrà rivolgersi direttamente all'OdV;

- un collaboratore esterno/ditta che presta la propria opera presso una delle aree di attività: può effettuare le segnalazioni al suo coordinatore o referente o in alternativa direttamente all'OdV;

- un esponente degli Organi sociali e del management, i collaboratori occasionali, i consulenti, i partner, ecc: potranno invece rivolgersi direttamente all'OdV.

Le segnalazioni dovranno avvenire in forma esplicita scritta attraverso l'applicazione messa a disposizione dei dipendenti e attraverso il sito www.altintech.it anche dei portatori di interesse esterni.
Il segnalante potrà così comunicare in forma anonima e gli è garantito che non avrà alcuna ritorsione derivante dalla segnalazione in oggetto.

L'OdV valuta le segnalazioni ricevute, effettua verifiche/approfondimenti, informa gli organi competenti delle risultanze delle verifiche effettuate.

4.5.2 Obblighi di informazione in relazione ad atti ufficiali

Oltre alle segnalazioni ufficiose di cui sopra, devono essere tempestivamente ed obbligatoriamente trasmesse all'OdV le informative concernenti:

- i provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i reati di cui al Decreto;

- le richieste di assistenza legale inoltrate dai dipendenti e/o dirigenti in caso di avvio di procedimento giudiziario per i reati previsti dal Decreto;

- i rapporti preparati dai responsabili di altre funzioni aziendali nell'ambito della loro attività di controllo e dai quali possano emergere fatti, atti, eventi od omissioni con profili di criticità rispetto all'osservanza delle norme sul Decreto;

- le notizie relative all'attuazione del Modello a tutti i livelli aziendali con evidenza dei procedimenti disciplinari e delle eventuali sanzioni irrogate (compresi i provvedimenti verso i dipendenti) ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni, se riferibili alla commissione dei reati previsti dal Decreto o a violazioni del Modello.

4.5.3 Sistema delle deleghe ed altra documentazione

All'OdV, infine, deve essere comunicato il sistema delle deleghe adottato da **ALTINTECH s.r.l.** ed ogni relativa modifica.

L'OdV dovrà inoltre ricevere copia delle **Schede di monitoraggio delle attività a rischio** istituite nelle Parti Speciali del presente Modello.

4.6 VERIFICHE ALL'ADEGUATEZZA DEL MODELLO

L'OdV è tenuto ad effettuare periodicamente verifiche in ordine alla reale capacità del Modello di prevenire la commissione egli illeciti ex D. Lgs. 231/01.

Tale attività si concretizza in:

- revisione della mappa delle aree a rischio in relazione alle modifiche nei processi e nell'organizzazione aziendale;
- analisi delle segnalazioni pervenute e relative azioni intraprese;
- verifica a campione di principali contratti / atti societari attinenti alle attività a rischio di reato ex D. lgs. 231/01;
- benchmarking con realtà analoghe;

Le verifiche effettuate e le proposte di adeguamento del Modello dovranno essere sintetizzate nel reporting al CdA.

5. SISTEMA DISCIPLINARE

5.1 INTRODUZIONE

I comportamenti sanzionabili in base al presente Modello sono individuabili in:

- adozione di comportamenti non conformi alle prescrizioni del Modello;
- violazione di procedure disciplinate dal presente Modello;
- adozione di comportamenti che possono configurare una delle ipotesi di reato previste dal presente Modello nell'ambito delle aree di attività a rischio;
- tentativi di violazione del Codice Etico qualora siano inequivocabili e gravi.

L'applicazione di provvedimenti o misure dovrà avvenire tenendo conto:

- della gravità, intenzionalità ed eventuale reiterazione del fatto;
- del grado di autonomia e responsabilità del soggetto che ha commesso il fatto;
- sempre e comunque nel rispetto della normativa vigente in materia di lavoro subordinato (es. Statuto dei Lavoratori), del Contratto Collettivo Nazionale e delle disposizioni aziendali.

5.2 SANZIONI NEI CONFRONTI DI LAVORATORI DIPENDENTI

I provvedimenti disciplinari applicabili al personale dipendente sono quelli previsti dal Contratto Collettivo Nazionale Metalmeccanico CONFAPI applicato da **ALTINTECH s.r.l.**, sempre nel rispetto dell'art. 7 dello Statuto dei Lavoratori, coerentemente con le procedure stabilite.
L'applicazione della sanzione verrà effettuata nel rispetto di tutte le disposizioni, previste dalla normativa e dal CCNL relativamente alle procedure ed obblighi da osservare.
Si applica la procedura interna: 3_06032017 ALTINTECH Srl Procedura Sanzioni Disciplinari ver.1.1,

5.3 SANZIONI NEI CONFRONTI DI SOGGETTI IN POSIZIONE APICALE O CHE RIVESTONO LA QUALIFICA DI DIRIGENTI

Nei confronti dei soggetti che rivestono la qualifica di dirigente o che ricoprono una posizione apicale, **ALTINTECH s.r.l.** applicherà le misure sanzionatorie idonee, in conformità del disposto normativo e del CCNL, considerando la particolarità del rapporto di carattere "fiduciario" e la necessità di ricorrere alla professionalità, disponibilità e competenza dei soggetti apicali.

5.4 MISURE NEI CONFRONTI DEGLI AMMINISTRATORI

In caso di violazione del Modello da parte dell'Amministratore, l'OdV è tenuto a informare tempestivamente i soci che prenderanno gli opportuni provvedimenti (es. convocazione CdA, revoca di deleghe, ecc.).

5.5 MISURE NEI CONFRONTI DEI SINDACI

Non è previsto collegio sindacale.

5.6 MISURE NEI CONFRONTI DI SOGGETTI ESTERNI

Con i soggetti esterni che hanno rapporti a qualsiasi titolo con **ALTINTECH s.r.l.** (committenti, clienti, fornitori, collaboratori, consulenti, partner, ecc.) che:

- pongano in essere comportamenti in violazione del presente Modello e del Codice Etico;
- agiscano in modo da comportare un effettivo rischio di commissione dei reati previsti dal D. Lgs. 231/01.

ALTINTECH s.r.l. ove possibile e in relazione alla tipologia di rapporto instaurato:

- risolverà detti rapporti;
- si impegnerà a non intraprenderne di nuovi con i medesimi soggetti;
- prevedrà apposite clausole contrattuali di risoluzione del contratto stesso.

5.7 IRROGAZIONE DELLE SANZIONI DISCIPLINARI

Le sanzioni saranno irrogate dai competenti organi / soggetti aziendali.

6. INDIVIDUAZIONE DELLE AREE AZIENDALI A RISCHIO

In questa fase sono state identificate le aree/settori di attività a rischio e la tipologia di reati previsti dal D. Lgs. 231/01.
Le fattispecie che rappresentano un effettivo rischio per **ALTINTECH s.r.l.** sono individuate nell'elenco seguente:

A) REATI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE

B) REATI SOCIETARI, inclusa CORRUZIONE TRA I PRIVATI (estesa dalla L. 190/12 nei casi previsti dall'art. 2635 c.c.)

C) REATI INFORMATICI inclusa FALSITA' IN DOCUMENTI INFORMATICI –(art.24-bis, D. Lgs 231/2001)

D) REATI COMMESSI IN VIOLAZIONE DELLE NORME ANTINFORTUNISTICHE E SULLA TUTELA DELL'IGIENE E DELLA SALUTE SUL LAVORO

E) RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA, NONCHÉ AUTORICICLAGGIO (art. 25-octies, d. lgs 231/01)

F) REATI AMBIENTALI

G) IMPIEGO DI CITTADINI DI PAESI TERZI IL CUI SOGGIORNO È IRREGOLARE (art. 25-doudecies)

A questi deve aggiungersi la fattispecie di *Abbandono e deposito incontrollati di rifiuti sul suolo e nel suolo* (prevista dall'art. 192, comma 4, D. Lgs. 152/2006), che determina una responsabilità della Società per la rimozione, l'avvio a recupero o lo smaltimento dei rifiuti e per il ripristino dello stato dei luoghi, in solido con il proprietario e con i titolari di diritti reali o personali di godimento sull'area, nel caso in cui il fatto illecito sia imputabile a suoi amministratori o rappresentanti, testualmente ricondotta alle "*previsioni del decreto legislativo 8 giugno 2001, n. 231, in materia di responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni*".

In applicazione del **criterio del c.d. "rischio accettabile"** si è dunque ritenuto di potere escludere dall'elenco delle tipologie di rischio-reato, le seguenti fattispecie:

- *falsità in monete, carte di pubblico credito e in valori di bollo* (art. 25-*bis* D. Lgs. n. 231/2001);
- reati *con finalità di terrorismo o di eversione dell'ordine democratico* (art 25-*quater* del D. Lgs. n. 231/2001);
- reati *contro la personalità individuale in materia di pornografia, integrità sessuale femminile e prostituzione minorile* (art 25-*quinquies* D. Lgs. n. 231/2001);
- *pratiche di mutilazione degli organi genitali femminili* (art 25-*quater* 1 D. Lgs. n. 231/2001);
- alcuni reati societari tra quelli previsti all'art. 25-*ter*, D. Lgs. n. 231/2001 (artt. 2623 c.c., commi 1 e 2 c.c.

- *falso in prospetto*; 2624, commi 1 e 2 c.c.
- *falsità nelle comunicazioni o nelle relazioni delle società di revisione*.

Queste tipologie di rischio verranno analizzate in dettaglio nella Parte Speciale dal punto A) al punto G).

Le Parti Speciali A) - G) del Modello hanno come obiettivo:

- l'individuazione delle aree di attività potenzialmente coinvolte nella fattispecie dei reati previsti dal Decreto;

- l'analisi dei reati contemplati dal D. Lgs 231/01 e dalla normativa specifica;

- l'indicazione delle procedure che gli Organi Sociali, i Dipendenti, i collaboratori esterni devono osservare ai fini di prevenire i reati in oggetto;

- l'individuazione degli strumenti di controllo da attribuire all'OdV ed ai responsabili delle funzioni aziendali.

SEZIONE II - PARTE SPECIALE A)

1. REATI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE

1.1 DEFINIZIONI DI PUBBLICA AMMINISTRAZIONE

La norma in ambito penale considera Ente della Pubblica Amministrazione “qualsiasi persona giuridica che abbia in cura interessi pubblici e che svolga attività legislativa, giurisdizionale o amministrativa in forza di norme di diritto pubblico e di atti autoritativi.”

Le figure che assumono particolare rilevanza ai sensi del D. Lgs. 231/01 non sono tuttavia tutti i dipendenti della P.A. ma in particolare i “Pubblici Ufficiali” e gli “Incaricati di Pubblico Servizio”.

1.2 DEFINIZIONI DI PUBBLICI UFFICIALI E INCARICATI DI PUBBLICO SERVIZIO

Pubblico ufficiale: l'art. 357 del Codice Penale definisce “Pubblico ufficiale” colui il quale “esercita una pubblica funzione legislativa, giudiziaria o amministrativa”. Inoltre viene definita “’pubblica’ la funzione amministrativa disciplinata da norme di diritto pubblico e da atti autoritativi e caratterizzata dalla formazione e dalla manifestazione della volontà della pubblica amministrazione o dal suo svolgersi per mezzo di poteri autoritativi o certificativi.”

Incaricato di pubblico servizio: secondo l'art. 358 del Codice Penale “sono incaricati di pubblico servizio coloro i quali, a qualunque titolo prestano un pubblico servizio. Per pubblico servizio deve intendersi un'attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri tipici di questa ultima, e con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale”.

1.3 TIPOLOGIE DI REATI

I reati previsti dal D. Lgs. 231/01 nei rapporti con la P.A. sono di seguito sintetizzati:

Malversazione a danno dello Stato e dell’Unione Europea (art. 316-bis c.p.)
Il reato viene attuato nel caso in cui un soggetto estraneo alla Pubblica Amministrazione, avendo ottenuto dallo stato o dal altro ente pubblico o dalle Comunità Europee contributi, sovvenzioni o finanziamenti destinati a favorire iniziative dirette alla realizzazione di opere od allo svolgimento di attività di pubblico interesse, non li destina alle finalità per cui erano erogati.
Il reato si configura con la mancata esecuzione dell’attività per cui sono stati erogati i finanziamenti ossia viene punita la mancata destinazione, anche parziale ed anche in riferimento a contributi ottenuti in passato, del finanziamento erogato allo scopo previsto.

Applicabilità

Tale rischio di reato può configurarsi nell'attività di **ALTINTECH s.r.l.**, che può richiedere e utilizzare finanziamenti pubblici (erogati direttamente o per il tramite di società terza capofila di ATI) sia a livello di organi direzionali che a livello operativo.
Il reato può configurarsi ad esempio utilizzando i fondi ricevuti per l'acquisto o la realizzazione di attività diverse rispetto a quelle di destinazione, manipolando i dati di rendicontazione in modo da far figurare spese sostenute per altri scopi, ecc.

Indebita percezione di erogazioni in danno dello Stato o dell'Unione Europea (art.316-ter c.p.)
Il reato si configura nei casi in cui, mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o mediante l'omissione di informazioni dovute, il soggetto consegue senza averne diritto, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo concessi o erogati dallo Stato, da altri enti pubblici o dalle Comunità europee.
Si precisa che in questa ipotesi non assume rilevo l'utilizzo che viene effettuato dei fondi, in quanto la fattispecie di reato si perfeziona al momento dell'ottenimento degli stessi.

Applicabilità

Tale rischio di reato può configurarsi nell'attività di **ALTINTECH s.r.l.** a livello di organi direzionali, ad esempio presentando documenti falsi o manipolati per attestare l'esistenza di condizioni di partecipazioni ad una gara.

Truffa aggravata in danno dello Stato, di altro ente pubblico o dell'Unione Europea (art. 640, comma 2 n.1, c.p.)
Il reato si configura qualora, per realizzare un ingiusto profitto, siano posti in essere artifici o raggiri tali da indurre in errore e da arrecare un danno allo Stato (oppure ad altro Ente Pubblico o all'Unione Europea).

Applicabilità

Tale ipotesi di reato può configurarsi in capo a **ALTINTECH s.r.l.** sia a livello di organi dirigenziali che a livello operativo (Amministrazione, Area commerciale) ad esempio falsificando i documenti di partecipazione ad una gara di appalto con lo Stato o ente pubblico, ponendo in essere una truffa per ottenere concessioni o contratti con la pubblica amministrazione, affidando forniture per acquisti in nome e per conto di Enti Pubblici (es. Ministeri) in violazione delle norme di legge.

Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.)
Il reato si configura qualora la truffa ai danni dello Stato di cui all'articolo precedente sia posta in essere per conseguire indebitamente erogazioni pubbliche.

Tale fattispecie può realizzarsi nel caso in cui si pongano in essere artifici o raggiri, ad esempio comunicando dati non veri o predisponendo una documentazione falsa, per ottenere finanziamenti pubblici.

Applicabilità

Tale ipotesi di reato può configurarsi in capo ad **ALTINTECH s.r.l.** sia a livello di organi dirigenziali che a livello operativo (principalmente Amministrazione, Area commerciale) ad esempio falsificando i documenti di partecipazione ad una gara con lo Stato o ente pubblico finalizzata ad ottenere erogazioni o finanziamenti, modificando artificiosamente le spese preventive da finanziare, rendicontando spese inesistenti, accordandosi con aziende capofila in progetti erogati da Enti Pubblici per ottenere illecitamente finanziamenti.

Frode informatica in danno dello Stato o altro ente pubblico (art. 640-ter c.p.)
Il reato si configura nel caso in cui, alterando il funzionamento di un sistema informatico o telematico o inserendo, cancellando o manipolando i dati in esso contenuti, si ottenga un ingiusto profitto arrecando danno a terzi.

Applicabilità

Tale ipotesi di reato può configurarsi in capo ad **ALTINTECH s.r.l.** sia a livello di organi dirigenziali che a livello operativo (principalmente Amministrazione) ad esempio alterando i dati del software di gestione della rendicontazione contributi, modificando dati previdenziali o fiscali già comunicati alla Pubblica Amministrazione anche per il tramite dei consulenti esterni (commercialista, consulente del lavoro, ecc.).
Tale ipotesi si può configurare anche per i software e servizi informatici che verranno acquistati in futuro.

Corruzione per un atto d'ufficio o contrario ai doveri d'ufficio (artt. 318-319-319 bis-320 c.p.)
Il reato si configura nel caso in cui un pubblico ufficiale (o incaricato di pubblico servizio) riceva, per sé o per altri, denaro o altri vantaggi per compiere, omettere o ritardare atti del suo ufficio ovvero per compiere atti contrari ai suoi doveri d'ufficio (determinando un vantaggio in favore dell'offerente).
Si differenzia dalla concussione in quanto in questa ipotesi di reato non c'è un abuso di un soggetto in virtù di una posizione o qualità ricoperta a danno dell'altro, ma un vantaggio reciproco delle parti.

Applicabilità

Tale reato può configurarsi in capo ad **ALTINTECH s.r.l.** principalmente in occasione delle trattative commerciali con la P.A., nella partecipazione a gare di appalto, nella stipula di convenzioni, nell'attività di rendicontazione contributi, ecc.
Può essere posta in essere mediante dazioni in qualsiasi forma o benefici quali promesse di assunzioni o favori a terzi.

Istigazione alla corruzione (art. 322 c.p.)
Il reato si configura qualora si pongano in essere atti o comportamenti finalizzati alla commissione del reato di corruzione ma il reato in sé stesso non si compie in quanto il pubblico ufficiale rifiuta l'offerta (o la promessa) illecitamente avanzatagli per indurlo a compiere od omettere o ritardare un atto del suo ufficio.

Applicabilità

Tale reato può configurarsi in capo ad **ALTINTECH s.r.l.** qualora si pongano in essere tentativi di corruzione in qualsiasi situazione nella quale il soggetto della PA sia un interlocutore con capacità decisionale o di spesa ma la corruzione non si compia in quanto l'offerta o promessa di dazioni non viene accettata dal pubblico ufficiale o incaricato di pubblico servizio.

Corruzione in atti giudiziari (art. 322 c.p.)
Il reato si configura nel caso in cui l'azienda sia coinvolta in un processo penale, amministrativo o civile e ponga in essere il reato di corruzione di pubblico ufficiale alfine di ottenere un vantaggio nel processo o procedimento stesso.

Applicabilità

Tale rischio di reato può configurarsi in capo ad **ALTINTECH s.r.l.** qualora, partecipando a processi civili – penali – amministrativi (es. fallimenti, cause civili o di lavoro, ecc.) nelle varie sedi, si tentasse di corrompere un pubblico ufficiale per ottenere un vantaggio per l'azienda. Il rischio sorge in capo principalmente ai legali rappresentanti della **ALTINTECH s.r.l.** o a coloro che hanno delega a rappresentarla in giudizio, ma è estensibile all'attività degli uffici di supporto.

1.4 AREE A RISCHIO

Sono definite "Aree a rischio" tutte le aree aziendali che, nella realizzazione delle proprie operazioni, interagiscono con la Pubblica Amministrazione. Inoltre, si definiscono "Aree di Supporto" le aree aziendali che svolgono attività tecnica/amministrativa di supporto che, pur non intrattenendo rapporti con la Pubblica Amministrazione, possono concorrere nella commissione dei reati.

Aree a rischio:

- Direzione;
- Legale e HR

Aree di supporto:

- Area commerciale
- Amministrazione
- Servizi tecnici

1.5 DESTINATARI DELLA PARTE SPECIALE

I destinatari della parte speciale relativa ai Reati nei rapporti con la P.A. sono:

- i Dirigenti;
- i dipendenti in linea gerarchica che operano nelle aree di attività a rischio;
- collaboratori esterni che operano per conto o con la **ALTINTECH s.r.l.**

1.6 PRINCIPI DI COMPORTAMENTO

Ai fini di prevenire che vengano commessi reati nei rapporti con la P.A., è espressamente fatto divieto ai destinatari della presente parte speciale di porre in essere:

- comportamenti tali da commettere o potenzialmente integrare le fattispecie di reato contemplate negli artt. 24 e 25 del D. Lgs. 231/01;

- qualsiasi situazione di conflitto di interesse nei confronti della Pubblica Amministrazione.

E' inoltre fatto divieto - coerentemente con quanto previsto nel Codice Etico - di:

- offrire doni, elargizioni e/o denaro a funzionari pubblici (italiani o stranieri) o a loro familiari tali da influenzare l'indipendenza di giudizio o indurre ad assicurare vantaggi per l'azienda e che travalichino l'ordinaria cortesia o prassi commerciale. Sono consentiti omaggi di minimo valore economico volti esclusivamente a promuovere iniziative di carattere benefico, artistico o culturale. Eventuali regali elargiti che superino il modico valore devono in ogni caso essere adeguatamente documentati ai fini delle opportune verifiche da parte dell'OdV;

- evitare che l'affidamento di incarichi di consulenza aziendale possa costituire l'oggetto dell'ingiusta retribuzione dei reati di corruzione;

- concedere favori di qualsiasi natura (promesse di assunzioni, cancellazione del debito verso enti impositori, ecc.) a rappresentanti della Pubblica Amministrazione a vantaggio proprio o di terzi;

- riconoscere compensi non commisurati al tipo di incarico da svolgere e dalle prassi vigenti in ambito locale, in favore dei collaboratori esterni;

- presentare dichiarazioni non veritiere ad organismi pubblici nazionali o comunitari al fine di conseguire erogazioni pubbliche, contributi o finanziamenti;

- destinare le erogazioni, contributi o finanziamenti ricevute da organismi pubblici nazionali o comunitari per scopi diversi da quelli cui erano destinati.

1.7 REGOLE DI CONDOTTA

Omaggi a pubblici ufficiali o incaricati di pubblico servizio:

- la procedura è sostanzialmente configurabile come un processo di acquisto e va articolata nelle seguenti fasi:

1. pianificazione e comunicazione del fabbisogno;
2. individuazione del fornitore e conseguente acquisizione;
3. gestione dell'erogazione dei beni/servizi (diretta e tramite magazzino);

- separazione di ruolo fra richiedente e acquirente dell'omaggio e definizione di specifiche soglie di valore per gli omaggi;

- identificazione dei soggetti aziendali titolati a rilasciare omaggi (richiedente), e a provvedere alla fornitura (acquirente);

- esistenza di specifici range economici, con espressa indicazione dei valori entro i quali l'omaggio è da considerarsi modesto;

- registrazione, presso la Direzione, degli omaggi consegnati a dipendenti della Pubblica Amministrazione;

- esistenza, presso i soggetti coinvolti, di evidenza documentale delle singole fasi del processo (richiesta, acquisto e consegna);

Rapporti di consulenza:

- la scelta del consulente (incluso il rappresentante o il difensore) avviene in relazione alle tematiche da gestire e sulla base di criteri di serietà, professionalità e stimata reputazione

- espletamento di adeguata attività selettiva fra diversi offerenti e di obiettiva comparazione delle offerte (sulla base di criteri oggettivi e documentabili
- la notula del consulente deve essere commisurata alla prestazione e in linea con gli accordi intrapresi;

- l'attività di consulenza sarà opportunamente documentata con cadenza periodica;

- l'attività di eventuali agenti, procacciatori, intermediari sarà opportunamente documentata con cadenza periodica;

- il consulente deve vincolarsi all'osservanza dei principi etico-comportamentali adottati dalla Società stessa;

- la Direzione deve comunicare all'OdV, con periodicità annuale: un piano annuale delle consulenze e relativi aggiornamenti periodici; il consuntivo attività di consulenza suddivise per fornitore;

Gestione del contenzioso:

- archiviazione di copia dei documenti ufficiali diretti (tramite legali esterni o periti di parte) a Giudici, a membri del Collegio Arbitrale, o a Periti d'ufficio chiamati a giudicare sul contenzioso di interesse della Società;

- valutazione di congruità formale dei flussi documentali e di esperibilità delle azioni funzionali al procedimento, da parte del presidio legale di riferimento;

- la Direzione deve comunicare all'OdV, per quanto di competenza e con periodicità definita: l'elenco contenziosi in corso e l'elenco dei contenziosi conclusi;

- il soggetto che riceve ogni eventuale notifica riguardante qualsiasi procedimento giudiziario o amministrativo deve tempestivamente consegnare anche alla Direzione copia dell'atto ricevuto confermandone tramite posta elettronica l'avvenuta consegna;

- il soggetto che riceve ogni rilevante missiva riguardante minaccia di procedimento giudiziario o amministrativo deve tempestivamente consegnare anche alla Direzione copia della missiva ricevuta confermandone tramite posta elettronica l'avvenuta consegna;

Gestione delle ispezioni svolte dalle autorità pubbliche, di vigilanza o di polizia giudiziaria:

- tempestiva e completa messa a disposizione dei documenti che gli incaricati della Guardia di Finanza, ASL, INAIL, INPS, o altro organo richiedente ritengano necessario acquisire nel corso delle attività ispettive;

- partecipazione alle ispezioni dei soli soggetti a ciò espressamente delegati - redazione e conservazione dei verbali formati in occasione dell'ispezione;

- il coinvolto nella verifica ne comunica l'inizio all'Organismo di Vigilanza, cui trasmette altresì copia del verbale conclusivo dell'ispezione;

SEZIONE II - PARTE SPECIALE B)

1. REATI Ssocietari

1.1 TIPOLOGIE DI REATI

- False comunicazioni sociali (artt. 2621, 2622 c.c.);
  formazione e redazione dei bilanci, delle relazioni o delle altre comunicazioni sociali previste dalla legge e dirette ai soci o al pubblico, esponendo fatti materiali non rispondenti al vero ovvero omettendo informazioni la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della Società.

- Impedito controllo (art. 2625, comma 2, c.c.);
  ostacolo al libero espletamento ed efficace svolgimento delle attività di controllo e di revisione, con particolare attenzione alla gestione dei rapporti con le società di revisione, con l'assemblea ed il collegio sindacale, nonché con le autorità pubbliche di vigilanza.

- Indebita restituzione dei conferimenti (art. 2626 c.c.);

- Operazioni in pregiudizio dei creditori (art. 2629 c.c.);
  operazioni (formazione o aumento fittizio di capitale sociale, acquisto o sottoscrizione di azioni da parte di amministratori, riduzioni del capitale sociale, fusioni o scissioni) che possono incidere:1) sulla formazione o sulla entità del capitale sociale alterandone fittiziamente l'entità mediante attribuzione di azioni o quote in misura superiore all'ammontare del capitale sociale o mediante sottoscrizione reciproca di azioni o quote ovvero sopravvalutando i conferimenti 2) sull'integrità del capitale sociale o delle riserve o che si risolvono in operazioni pregiudizievoli per i creditori.

- Illegale ripartizione degli utili e delle riserve (art. 2627 c.c.);
  operazioni relative:1) alla ripartizione di utili non effettivamente conseguiti o alla distribuzione di utili destinati per legge a riserve, o alla ripartizione di riserve, all'acquisto o sottoscrizione di azioni o quote da parte degli amministratori sia della Società di appartenenza che della Società controllante, che cagionino una lesione all'integrità del capitale sociale o delle riserve non disponibili 2) a restituzioni anche simulate di conferimenti al di fuori dei casi di legittima riduzione del capitale sociale e ove questa sia contabilmente possibile.

- Illecita influenza sull'assemblea (art. 2636 c.c.);
  formazione delle maggioranze assembleari con indebita influenza che possa derivare da atti simulati o fraudolenti.

1.2 DESTINATARI DELLA PARTE SPECIALE

I destinatari della parte speciale sono:

- Direzione

- soci
- i dipendenti in linea gerarchica che operano nelle aree di attività a rischio
- collaboratori esterni che operano per conto o con la società

Attività a rischio:

- Amministrazione, Contabilità

1.3 PRINCIPI DI COMPORTAMENTO

E' vietato agli organi **ALTINTECH s.r.l.**, ai dipendenti, ai consulenti/collaboratori nella misura necessaria alle funzioni dagli stessi svolte di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, la fattispecie di reato in esame;
- violare i principi e le procedure esistenti in materia di amministrazione contabile.

1.4 ATTIVITA' SPECIFICHE IN RIFERIMENTO ALLE OPERAZIONI A RISCHIO

Ai fini del presente Modello l'attività dell'area Amministrazione è particolarmente significativa, specie in rapporto alla gestione della contabilità e della fatturazione (attiva e passiva) dove potrebbero realizzarsi condotte volte alla violazione della normativa in materia societaria.

In particolare, tali condotte potrebbero determinare una falsificazione delle comunicazioni sociali, nel caso in cui i dati alterati concernenti la fatturazione passiva fossero poi inseriti nel bilancio della **ALTINTECH s.r.l.** o in altre comunicazioni sociali rilevanti, integrando un'esposizione di fatti non rispondenti al vero idonea ad indurre in errore soci o creditori sulla situazione economica, patrimoniale o finanziaria della Società stessa. Inoltre, tali condotte potrebbero produrre conseguenze rilevanti in ordine ad eventuali operazioni sul capitale sociale in pregiudizio ai creditori.

Eventuali violazioni della normativa societaria e dei principi di contabilità potrebbero poi svolgere un ruolo strumentale rispetto alla commissione di reati in tema di ricettazione, riciclaggio e impiego di beni di provenienza illecita, nonché di autoriciclaggio ovvero di reati transnazionali, o anche di reati contro la pubblica amministrazione, specie ove servissero a costituire fondi neri da utilizzare come corrispettivi di attività corruttive.

Nel caso in cui le attività sopra descritte comportino la redazione di un documento informatico, intendendosi come tale – secondo la definizione contenuta nell'art. 491-bis c.p. il cui riferimento è peraltro venuto meno a seguito dell'intervento della l. 48/2008 - "qualsiasi supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli" ovvero la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti (come stabilito invece dall'art. 1, lett. a), D.P.R. 513/1997) e come "supporto informatico" qualsiasi "supporto di memoria – sia esso interno o esterno all'elaboratore – sul quale possono essere registrati e conservati per un certo lasso di tempo dei dati, destinati ad essere letti ed eventualmente elaborati da un sistema

informatico", potrebbero infine commettersi reati in tema di falsità di documenti informatici.

1.5 I CONTROLLI DELL'ODV

In merito a quanto disciplinato nella presente parte speciale, l'OdV ha i seguenti compiti:

- verificare periodicamente l'osservanza delle disposizioni di legge e delle procedure interne;

- analizzare le eventuali segnalazioni provenienti dai destinatari del Modello in merito al rispetto della normativa di amministrazione contabile.

1.6 REGOLE DI CONDOTTA

In considerazione dei rischi sopra specificati, la **ALTINTECH s.r.l.** ha predisposto un sistema di regole e procedure.

Nello specifico, con riferimento all'**attività contabile**, sono state individuate le seguenti regole comportamentali:

- L'attività amministrativa e contabile della Società (fatturazione attiva e passiva) è gestita attraverso i sistemi informatici;
- Ogni acquisto è supportato da documentazione cartacea;
- Ogni pagamento viene bloccato automaticamente qualora non sia presente un ordine d'acquisto;
- L'azienda pianifica il conto economico e lo stato patrimoniale anche in relazione alla pianificazione annuale e formula conti economici previsionali;
- Il controllo di gestione comporta un periodico (mensile) raccordo fra preventivo e consuntivo, spiegando e motivando i disallineamenti, con contestuale e consequenziale riformulazione delle previsioni.

La riconciliazione dei dati contabili viene periodicamente ripetuta allo scopo di evitare disallineamenti che possano tradursi in vere e proprie anomalie di bilancio.

Il sistema complessivo risulta dunque affidato ad un meccanismo di contrappesi e di reciproci controlli che rendono oltremodo improbabile la realizzazione di reati del tipo considerato, se non attraverso una elusione fraudolenta realizzata da una pluralità di agenti in accordo fra loro. La registrazione di dati e documenti a rilevanza contabile (ad es. fatture, note di credito, note di debito, pagamenti, incassi, etc.) avviene a mezzo di appositi e dedicati sistemi informatici.

L'OdV si riunisce almeno una volta all'anno, in prossimità della riunione del C.d.A., per l'approvazione del progetto di bilancio, con il collegio sindacale al fine di verificare tale documento; della riunione è redatto apposito verbale.

In relazione **all'inventario di magazzino** si osservano le seguenti regole di condotta: l'inventario annuale viene predisposto e sottoscritto da più soggetti con uno

scarto tra le giacenze reali e quelle calcolate non superiore al 15%.

Si osservano le seguenti regole di condotta per gli **omaggi**:

- definizione di specifiche soglie di valore per gli omaggi;
- identificazione dei soggetti aziendali titolati a rilasciare omaggi (richiedente), e a provvedere alla fornitura (acquirente);
- esistenza di specifici range economici, con espressa indicazione dei valori entro i quali l'omaggio è da considerarsi modesto;
- esistenza di un "catalogo" delle tipologie di beni/servizi che possono essere concessi come omaggio (agende, calendari, oggetti sociali, abbonamenti, ecc.);

Nella **fissazione dei prezzi (e degli sconti)** dei beni si osservano le seguenti regole:

- il calcolo per l'applicazione del prezzo e della scontistica deve esser documentato e archiviato;

Sui **rapporti di consulenza,** si osservano le seguenti regole di condotta, specie al fine di evitare che l'affidamento di incarichi di consulenza aziendale possa costituire l'oggetto dell'ingiusta retribuzione dei reati di corruzione:

- la scelta del consulente (incluso il rappresentante o il difensore) avviene in relazione alle tematiche da gestire e sulla base di criteri di serietà, professionalità e stimata reputazione;
- espletamento di adeguata attività selettiva fra diversi offerenti e di obiettiva comparazione delle offerte (sulla base di criteri oggettivi e documentabili);
- la notula del consulente deve essere commisurata alla prestazione e in linea con gli accordi intrapresi;
- il consulente deve vincolarsi all'osservanza dei principi etico-comportamentali adottati dalla Società stessa.

Con il riferimento **ai pagamenti** si osserva quanto stabilito nella sezione relativa ai reati di ricettazione, riciclaggio, autoriciclaggio ed impiego di denaro o altra utilità.

In relazione alla **selezione e gestione del personale**, oltre alle procedure già adottate dalla Società, si osservano le seguenti regole di condotta:

- **ALTINTECH s.r.l.** osserva le normative anticorruzione anche ai fini delle nuove assunzioni, delle promozioni e delle valutazioni dei candidati da selezionare e da inserire nell'organico aziendale;
- ogni richiesta di assunzione deve essere accompagnata da apposita documentazione (dossier);

ALTINTECH s.r.l. comunica alla società incaricata del servizio di elaborazione paghe e stipendi del personale l'avvenuta adozione del presente modello organizzativo e ne rilascia copia per presa visione, garantendone il rispetto anche da parte di questa, nell'esercizio delle funzioni individuate nel contratto di fornitura.

2. REATO DI CORRUZIONE TRA PRIVATI

Corruzione tra i privati (estesa dalla L. 190/12 nei casi previsti dall'art. 2635 c.c.)

Sono soggetti attivi del reato:

A) amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari, sindaci, liquidatori di una società;

B) coloro che sono sottoposti alla direzione e alla vigilanza dei soggetti indicati al precedente punto A).

Il reato si configura quando il soggetto attivo, a seguito della dazione o della promessa di denaro o altra utilità, per sé o per altri, compie o omette atti, in violazione degli obblighi inerenti al suo ufficio o degli obblighi di fedeltà, in nocumento alla società cui appartiene.

Il reato è sanzionato con la pena da 1 a 3 anni per i soggetti di cui al punto A) e reclusione fino a 1 anno e 6 mesi per i soggetti di cui al punto B).
Le stesse pene sono previste a carico di chi dà o promette denaro o altra utilità. La pena è raddoppiata se la società "danneggiata" è quotata in Italia o in un altro Stato dell'UE (non è il caso della **ALTINTECH s.r.l.** alla data).

Il reato è procedibile a querela della persona offesa (cioè la società che subisce il danno) ma anche d'ufficio se dal fatto deriva una distorsione della concorrenza nell'acquisizione di beni o servizi.
La corruzione tra privati è reato-presupposto della responsabilità amministrativa ex D. Lgs. 231/2001, e costituisce fonte di responsabilità per l'ente di appartenenza dell'autore della corruzione. La responsabilità sarà limitata all'ente del quale è esponente il corruttore. Potrà dunque configurarsi la responsabilità dell'ente nell'ipotesi in cui il corruttore (soggetto apicale o "sottoposto") dia o prometta denaro o altra utilità alle persone indicate nel primo e nel secondo comma dell'articolo 2635 c.c. appartenente a un'altra società nell'interesse o a vantaggio dell'ente di appartenenza.

Applicabilità
Tale reato può configurarsi in capo a **ALTINTECH s.r.l.** qualora il soggetto appartenente a un'altra società sia un interlocutore con capacità decisionale o di spesa.

2.1 AREE A RISCHIO

Sono definite "Aree a rischio" tutte le aree aziendali che, nella realizzazione delle proprie operazioni, interagiscono con soggetti commerciali esterni. Inoltre, si definiscono "Aree di Supporto" le aree aziendali che svolgono attività tecnica/amministrativa di supporto che, pur non intrattenendo rapporti diretti con soggetti commerciali esterni, possono concorrere nella commissione dei reati.

Aree a rischio:

- Direzione;
- Amministrazione;
- Responsabili di commessa;

2.2 DESTINATARI DELLA PARTE SPECIALE

I destinatari della parte speciale relativa al reato di corruzione tra privati sono:

- i Dirigenti;
- i dipendenti in linea gerarchica che operano nelle aree di attività a rischio;
- collaboratori esterni che operano per conto o con la **ALTINTECH s.r.l.**

2.3 PRINCIPI DI COMPORTAMENTO

Ai fini di prevenire che venga commesso questo reato, è espressamente fatto divieto ai destinatari della presente parte speciale - coerentemente con quanto previsto nel Codice Etico - di:

- offrire o promettere doni, elargizioni e/o denaro;

- concedere favori di qualsiasi natura (promesse di assunzioni, cancellazione del debito commerciale, ecc.);

- riconoscere compensi non commisurati al tipo di incarico da svolgere e dalle prassi vigenti in ambito locale, in favore dei collaboratori esterni;

SEZIONE II - PARTE SPECIALE C)

1. REATI INFORMATICI

1.1 TIPOLOGIE DI REATI

In considerazione delle attività oggi svolte dalla **ALTINTECH s.r.l.** si riporta l'elenco dei comportamenti che, ai sensi dell'art. 24 del D. Lgs. 231/01, introdotto dal D. Lgs. n. 121 del 7 luglio 2011 e in vigore dal 16 agosto 2011, possono determinare una responsabilità dell'ente.

- Frode informatica;
- Falsità in un documento informatico pubblico o avente efficacia probatoria (Art.491-bis C.P.,)
- Accesso abusivo ad un Sistema informatico o telematico (Art. 615-ter C.P.)
- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (Art. 615-quater C.P.)
- Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (Art. 615-quinquies C.P.)
- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (Art. 617-quater)
- Trattamento illecito di dati, falsità nelle dichiarazioni e notificazioni al Garante della privacy, inosservanza delle misure minime di sicurezza e di protezione dei dati personali (artt. 167 - 172 D. Lgs. n. 196/2003 – Regolamento Europeo 16/679).
- Danneggiamento di informazioni, dati e programmi informatici. (Art. 635-bis)
- Danneggiamento di sistemi informatici o telematici. (Art. 635-quater)

In sostanza, tutte le attività implicanti la redazione di un documento informatico, intendendosi come tale “qualsiasi supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli” e come “supporto informatico” qualsiasi “supporto di memoria – sia esso interno o esterno all’elaboratore – sul quale possono essere registrati e conservati per un certo lasso di tempo dei dati, destinati ad essere letti ed eventualmente elaborati da un sistema informatico”, possono essere rilevanti penalmente ai sensi dell’art. 491 bis c.p. in chiave di reato presupposto.

Inoltre, assumono astrattamente rilevanza in chiave di possibili reati presupposto, tutte le attività che si svolgono mediante sistemi informatici interni adottati dalla Società, con particolare riferimento a:

- comunicazioni telematiche o informatiche dirette alla Pubblica Amministrazione;
- comunicazioni telematiche od informatiche, in generale, ad ogni autorità pubblica che intrattenga rapporti con la Società;
- accesso alla rete aziendale;
- abilitazione all'accesso, manutenzione e custodia della password;
- scambio corrispondenza interna via telematica;
- corrispondenza con l'esterno tramite posta elettronica;
- lettura della corrispondenza in caso di assenza del dipendente;
- manutenzione dei sistemi, dei terminali e dei PC dei dipendenti;
- interruzioni nelle comunicazioni e nelle operazioni d'uso dei PC;
- predisposizione, modificazione, trasmissione, archiviazione e custodia di dati, informazioni o documenti per via o su supporto telematico o informatico;

1.2 DESTINATARI DELLA PARTE SPECIALE

I destinatari della parte speciale sono:

- Direzione;
- Amministrazione;
- Area Tecnica;
- Tutti coloro che a vario titolo lavorano per conto e con **ALTINTECH s.r.l.**

1.3 PRINCIPI DI COMPORTAMENTO

Sono rilevanti in questa sede i dispositivi di sicurezza dei sistemi informatici utilizzati nell'azienda nonché i principi generali che informano l'attività informatica già indicati nel Regolamento per la Protezione dei Dati. Tale documento interno adatta le disposizioni del Garante per il trattamento dei dati personali in materia di riservatezza ("Linee Guida del Garante per posta elettronica ed internet") ai processi aziendali, garantendo inoltre una corretta organizzazione ed un'adeguata prevenzione nei confronti dei reati informatici.

Per quanto attiene alla nuova normativa dell'art.4 dello Statuto dei Lavoratori - Jobs Act 2015, relativa alle misure in materia di controllo a distanza dei lavoratori, il riferimento legislativo è il D. Lgs 151/2015 "Disposizioni di razionalizzazione e semplificazione delle procedure e degli adempimenti a carico di cittadini e imprese e altre disposizioni in materia di rapporto di lavoro e pari opportunità", articolo 23, a modifica dell'art. 4 dello Statuto dei lavoratori: *"Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo gli impianti e gli strumenti di cui al periodo precedente possono essere installati previa autorizzazione della Direzione territoriale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più Direzioni territoriali*

del lavoro, del Ministero del lavoro e delle politiche sociali.“
Si precisa che tale disposizione *“non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze“*.
Quindi *“le informazioni raccolte ai sensi del primo e del secondo comma sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d’uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196“.*
Unico limite indicato dal legislatore, o meglio ricordato dal legislatore al terzo comma, il rispetto delle prescrizioni di informazione con un richiamo al decreto legislativo 196 del 2003, il cosiddetto Codice Privacy, secondo il quale gli elementi che il datore di lavoro andrà a raccogliere, nel rispetto del primo e del secondo comma dell’articolo 4, potranno essere utilizzabili per tutti i fini connessi al rapporto lavorativo. Questo a condizione che, al lavoratore, venga fornita informazione sulle modalità di uso degli strumenti e dei consequenziali controlli. Informazione che, congruamente alla ratio del Codice Privacy, dovrà essere resa preventivamente al trattamento dei dati del dipendente che potrà essere realizzato.

1.4 REGOLE SPECIALI DI CONDOTTA

È vietato porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle qui considerate; sono altresì proibite le violazioni ai principi ed alle procedure aziendali previste nella presente Parte Speciale.

Fermo restando quanto sopra i Destinatari del presente Modello devono attenersi alle seguenti condotte:

- osservare rigorosamente tutte le leggi e i regolamenti e procedure in materia di privacy;
- partecipare ai corsi aziendali in materia;
- segnalare alle funzioni competenti eventuali criticità che possono creare rischi;
- fornitori e gli altri Destinatari esterni alla **ALTINTECH s.r.l.** devono dare evidenza del rispetto da parte loro delle normative di riferimento;

1.5 I CONTROLLI DELL’ODV

In merito a quanto disciplinato nella presente parte speciale, l’OdV ha i seguenti compiti:

- verificare periodicamente l’osservanza delle disposizioni di legge e delle procedure aziendali;
- analizzare le eventuali segnalazioni provenienti dai destinatari del Modello in merito al rispetto della normativa sulla sicurezza del lavoro.

SEZIONE II - PARTE SPECIALE D)

1. REATI IN VIOLAZIONE DELLE NORME ANTINFORTUNISTICHE E SULLA TUTELA DELL'IGIENE E DELLA SALUTE SUL LAVORO

1.1 TIPOLOGIE DI REATI

In considerazione delle attività oggi svolte dalla **ALTINTECH s.r.l.** nonché del documento di valutazione dei rischi predisposto ai sensi del D. Lgs 81/2008 e s.m.i., le attività a rischio per le quali potrebbero ravvisarsi gli estremi per la commissione dei reati in discussione sono limitate e riconducibili:

- allo svolgimento di attività lavorative presso la sede operativa con utilizzo di scrivanie e videoterminali;

- allo svolgimento di attività lavorative all'esterno, presso cantieri temporanei o presso presidi tecnici messi a disposizione dai committenti;

1.2 DESTINATARI DELLA PARTE SPECIALE

I destinatari della parte speciale relativa ai reati di omicidio colposo e lesioni colpose gravi e gravissime, commesse con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro sono:

- Datore di lavoro;
- Organizzazione aziendale per la prevenzione e protezione;
- Legale e HR
- i dipendenti;
- tutti coloro che a vario titolo lavorano per conto e con **ALTINTECH s.r.l.**

1.3 PRINCIPI DI COMPORTAMENTO

È vietato porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle qui considerate; sono altresì proibite le violazioni ai principi ed alle procedure aziendali previste nella presente Parte Speciale.

Al fine di evitare il verificarsi dei reati di omicidio colposo e lesioni colpose gravi e gravissime, previsti dal Decreto Legislativo n. 231/01, tutti i Destinatari del presente Modello devono attenersi alle specifiche regole e procedure che sono e saranno predisposte dal Datore di Lavoro e dal Responsabile del Servizio di Prevenzione e Protezione istituito ai sensi del D. Lgs. 81/2008 e s.m.i. e diffuse dal Responsabile del Sistema di Protezione e Prevenzione.

Questa parte del Modello si integra con quanto previsto dal Sistema di Gestione della Sicurezza SGS sviluppato in azienda secondo lo standard OHSAS 18001.

Fermo restando quanto sopra i Destinatari del presente Modello devono attenersi alle seguenti condotte:

- osservare rigorosamente tutte le leggi e i regolamenti e procedure in materia di sicurezza sul lavoro e sulla tutela dell'igiene e salute sul lavoro che disciplinano l'accesso, il transito e lo svolgimento delle attività lavorative presso i locali aziendali e quelli in uso temporaneo;
- partecipare ai corsi aziendali in materia di sicurezza sul lavoro e sulla tutela dell'igiene e salute sul lavoro, ecologia e sullo svolgimento delle specifiche mansioni, ai quali saranno invitati;
- in funzione delle mansioni svolte, utilizzare dispositivi di protezione forniti dalla azienda e conformi alle normative vigenti;
- segnalare alle funzioni competenti eventuali inefficienze dei dispositivi di protezione individuali ovvero di altri presidi a tutela della sicurezza sul lavoro e sulla tutela dell'igiene e salute sul lavoro.
- Fornitori e gli altri Destinatari esterni alla **ALTINTECH s.r.l.** devono dare evidenza del rispetto da parte loro delle normative sulla sicurezza sul lavoro e sulla tutela dell'igiene e salute sul lavoro;

1.4 ATTIVITA' SPECIFICHE IN RIFERIMENTO ALLE OPERAZIONI A RISCHIO

Al fine di tutelare la sicurezza, salute e igiene sul lavoro, in linea con le previsioni del D. Lgs 81/2008 e s.m.i., sono previste specifiche procedure, secondo lo standard internazionale OHSAS 18001 per la quale la **ALTINTECH s.r.l.** è certificata da ente terzo, in forza delle quali:

- sono periodicamente individuati dal Datore di Lavoro e dal Responsabile del Servizio Prevenzione e Protezione i rischi in materia di sicurezza e tutela dell'igiene e salute sul lavoro, tenendo in adeguata considerazione la struttura aziendale, la natura delle attività, l'ubicazione dei locali e delle aree di lavoro e l'organizzazione del personale. Nella valutazione dei rischi adottano criteri oggettivi, documentati e ripetibili, considerando, per ogni specifico rischio, la probabilità di accadimento, la dimensione dell'impatto del danno possibile, i risultati di rilievi ambientali e la storia degli infortuni verificatisi nello svolgimento della specifica attività;

- viene aggiornato, periodicamente ed in occasione di significative modifiche organizzative, il documento di valutazione dei rischi, redatto ai sensi del D. Lgs. 81/2008 e s.m.i.;

- il Datore di Lavoro e il Responsabile del Servizio Prevenzione e Protezione rivedono periodicamente il piano di intervento delle azioni di prevenzione e protezione sulla base del risultato della valutazione dei rischi, nonché i programmi di informazione e formazione dei lavoratori ai fini della sicurezza e della protezione della loro salute;

- i Destinatari del presente Modello sono tenuti a sorvegliare sull'effettivo rispetto delle procedure e sulla adozione delle adeguate misure di prevenzione e protezione, comunicando tempestivamente in primis al Datore di Lavoro e/o al Responsabile del

Servizio di Prevenzione e Protezione e soltanto in caso di inerzia di questi ultimi all'OdV, eventuali eccezioni e criticità;

- è definito il metodo di segnalazione e comportamento da tenere in caso di emergenze;

- i lavoratori in base agli specifici rischi individuati a cui sono soggetti ricevono adeguata informazione e formazione in merito alla misure di prevenzione e protezione da adottare nello svolgimento delle proprie attività e gestione delle emergenze,

- alle ispezioni giudiziarie e amministrative devono partecipare i soggetti a ciò espressamente delegati. L'OdV dovrà essere prontamente informato sull'inizio di ogni attività ispettiva e sull'evoluzione delle stesse. Copia dei verbali dell'ispezione devono essere conservati dall'OdV;

- sono previsti obblighi di riporto periodico all'OdV con riguardo a quanto previsto dal presente modello.

1.5 I CONTROLLI DELL'ODV

In merito a quanto disciplinato nella presente parte speciale, l'OdV ha i seguenti compiti:

- verificare periodicamente l'osservanza delle disposizioni del Decreto e delle procedure aziendali in tema di sicurezza del lavoro;

- analizzare le eventuali segnalazioni provenienti dai destinatari del Modello in merito al rispetto della normativa sulla sicurezza del lavoro.

SEZIONE II - PARTE SPECIALE E)

1. RICETTAZIONE, RICICLAGGIO, IMPIEGO DI DENARO, BENI O UTILITA' DI PROVENIENZA ILLECITA, NONCHE' AUTORICICLAGGIO

1.1 TIPOLOGIE DI REATI

In considerazione delle attività oggi svolte dalla **ALTINTECH s.r.l.** si riporta la fattispecie rilevante**:** ricettazione (art. 648 c.p.), riciclaggio (art. 648-bis c.p.), impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.), autoriciclaggio (art. 648-ter 1 c.p.).

Le fattispecie criminose considerate in questa sezione hanno un ampio spettro applicativo, che va dall'acquisto, recezione od occultamento di proventi delittuosi, fino alla sostituzione o al trasferimento degli stessi proventi o ad altre operazioni, non meglio specificate dalla legge, che ne ostacolino l'identificazione e al reimpiego in attività economiche o finanziarie di beni o altre utilità provenienti da delitto.

1.2 DESTINATARI DELLA PARTE SPECIALE

I destinatari della parte speciale sono:

- Direzione;
- Amministrazione;
- Tutti coloro che a vario titolo lavorano per conto e con **ALTINTECH s.r.l.**

Attività a rischio:

- Acquisto-vendita beni o servizi
- Pagamenti a terzi (fornitori e clienti)

1.3 PRINCIPI DI COMPORTAMENTO

E' vietato agli organi sociali, ai dipendenti, ai consulenti/Partner nella misura necessaria alle funzioni dagli stessi svolte di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, la fattispecie di reato in esame;
- violare i principi e le procedure esistenti in azienda in materia di assunzione del personale.

1.4 ATTIVITA' SPECIFICHE IN RIFERIMENTO ALLE OPERAZIONI A RISCHIO

L'apertura di qualsiasi conto corrente bancario necessita di autorizzazione secondo procedura standard;

In relazione all'**acquisto o vendita beni e servizi**, ad integrazione delle procedure del sistema qualità certificato, si osservano le seguenti regole di condotta:

- distinzione del processo in diverse fasi (richiesta di acquisto, ordine di acquisto, fornitura del bene o servizio, fatturazione), come previsto dalle procedure del sistema qualità;

- tutti gli ordini di acquisto di beni e servizi sono soggetti a procedura di approvazione con relativa archiviazione dell'elenco delle autorizzazioni riguardanti le richieste di acquisto;

- le spese che possono essere gestite senza ordine di acquisto (carte carburante, spese di viaggio, acquisti di valore modesto, spese di ospitalità) sono specificamente individuate;

- tutti i movimenti relativi alla piccola cassa sono debitamente registrati;

- esistenza e puntuale utilizzo di criteri tecnico-economici per la selezione di potenziali fornitori (qualificazione e inserimento in un Elenco Fornitori);

- espletamento di adeguata attività selettiva fra diversi offerenti e di obiettiva comparazione delle offerte (sulla base di criteri oggettivi e documentabili);

- utilizzo di idonei modelli contrattuali con termini e condizioni adeguatamente formalizzati;

- esistenza di livelli di approvazione per le richieste di acquisto e per la certificazione della fornitura/erogazione;

- esistenza di diversi livelli autorizzativi (in coerenza con il sistema delle procure aziendali) per la stipulazione, modifica ed estinzione dei rapporti contrattuali;

- tracciabilità delle singole fasi del processo (documentazione a supporto, livello di formalizzazione e modalità/tempistiche di archiviazione), per consentire la ricostruzione delle responsabilità, delle motivazioni delle scelte e delle fonti informative;

- verifica che la fornitura di beni o di servizi sia avvenuta a condizioni di mercato;

- la Direzione deve comunicare, per quanto di competenza e con periodicità definita, l'elenco degli acquisti effettuati in deroga ai requisiti sopra esposti;

- a qualunque livello, il soggetto responsabile della ricezione del bene o servizio verifica la congruità tra ordine di acquisto emesso e la precedente richiesta di acquisto dell'unità che necessitava del bene o servizio;

- l'inserimento e la modifica dei dati relativi ai fornitori sono effettuati in base ad apposite procedure anche con indicazione di fornitori collegati o meno alla P.A. o altri enti governativi;

In relazione ai **pagamenti**, si osservano le seguenti regole di condotta:

- esistenza di soggetti distinti che operino nelle seguenti fasi/attività del processo (richiesta della disposizione di pagamento per assolvere l'obbligazione; effettuazione del pagamento; controllo/riconciliazioni a consuntivo);

- esistenza di livelli autorizzativi sia per la richiesta di pagamento che per la disposizione, articolati in funzione dell'importo;

- esistenza di un flusso informativo sistematico che garantisca il costante allineamento fra poteri, procure e deleghe operative e profili autorizzativi residenti nei sistemi informativi;

- nessun pagamento può essere ricevuto dalla Società in contanti in deroga alle norme vigenti in materia, salvo espressa e speciale autorizzazione;

- nessun pagamento può essere effettuato oppure ricevuto dalla Società su conti bancari aperti all'estero tramite intermediari stranieri;

- ogni pagamento, inclusi quelli di cui a fatture, tasse, imposte e contributi, viene effettuato solo se autorizzato;

- per tutti i pagamenti ed altre utilità a favore della P.A., enti governativi, soggetti correlati, funzionari pubblici, intermediari di vendita devono essere predisposti con apposita documentazione attestante il tipo di operazione compiuta e relativa archiviazione;

- ogni pagamento deve essere effettuato solo se a favore di fornitore approvato e a seguito della registrazione di regolare fattura;

- i listini prezzi, la scontistica, i termini di pagamento sono stabiliti secondo procedure, sono prestabiliti e non modificabili;

- tutti i pagamenti a favore della P.A, enti governativi, soggetti correlati, funzionari pubblici sono monitorati;

- le istruzioni alla banca per bonifico a terzi devono essere redatte in lettera accompagnatoria con la descrizione della causale, e tale lettera deve essere tempestivamente archiviata;

1.5 I CONTROLLI DELL'ODV

In merito a quanto disciplinato nella presente parte speciale, l'OdV ha i seguenti compiti:

- verificare periodicamente l’osservanza delle disposizioni di legge e delle procedure aziendali;

- analizzare le eventuali segnalazioni provenienti dai destinatari del Modello in merito al rispetto della normativa del lavoro.

SEZIONE II - PARTE SPECIALE F)

1. REATI AMBIENTALI

1.1 TIPOLOGIE DI REATI

In considerazione delle attività oggi svolte dalla **ALTINTECH s.r.l.** si riporta l'elenco dei comportamenti che, ai sensi dell'art. 25-undecies (Reati ambientali) del D. Lgs. 231/01, introdotto dal D. Lgs. n. 121 del 7 luglio 2011 e in vigore dal 16 agosto 2011, possono determinare una responsabilità dell'ente.

D. Lgs 152/06, art. 256 - Attività di gestione di rifiuti non autorizzata
Comma 1
Chiunque effettua una attività di raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione di rifiuti in mancanza della prescritta autorizzazione, iscrizione o comunicazione di cui agli articoli 208, 209, 210, 211, 212,214, 215 e 21 è punito:
a) con la pena dell'arresto da tre mesi a un anno o con l'ammenda da duemilaseicento euro a ventiseimila euro se si tratta di rifiuti non pericolosi;
b) con la pena dell'arresto da sei mesi a due anni e con l'ammenda da duemilaseicento euro a ventiseimila euro se si tratta di rifiuti pericolosi.
Sanzione pecuniaria fino a duecentocinquanta quote (lett. a) o da centocinquanta a duecentocinquanta quote (lett. b). La sanzione è ridotta della metà "nelle ipotesi di inosservanza delle prescrizioni contenute o richiamate nelle autorizzazioni, nonché nelle ipotesi di carenza dei requisiti e delle condizioni richiesti per le iscrizioni o comunicazioni." (D. Lgs. 152/06, art. 256, co. 4).

Comma 3
Chiunque realizza o gestisce una discarica non autorizzata è punito con la pena dell'arresto da sei mesi a due anni e con l'ammenda da duemilaseicento euro a ventiseimila euro. Si applica la pena dell'arresto da uno a tre anni e dell'ammenda da euro cinquemiladuecento a euro cinquantaduemila se la discarica è destinata, anche in parte, allo smaltimento di rifiuti pericolosi. Alla sentenza di condanna o alla sentenza emessa ai sensi dell'articolo 444 del codice di procedura penale, consegue la confisca dell'area sulla quale è realizzata la discarica abusiva se di proprietà dell'autore o del compartecipe al reato, fatti salvi gli obblighi di bonifica o di ripristino dello stato dei luoghi.
Sanzione pecuniaria da centocinquanta a duecentocinquanta quote (primo periodo) e da duecento a trecento quote (secondo periodo). La sanzione è ridotta della metà "nelle ipotesi di inosservanza delle prescrizioni contenute o richiamate nelle autorizzazioni, nonché nelle ipotesi di carenza dei requisiti e delle condizioni richiesti per le iscrizioni o comunicazioni." (D. Lgs. 152/06, art. 256, co. 4). Nel caso di condanna (per le ipotesi previste dal secondo periodo) si applicano le sanzioni interdittive per una durata non superiore a sei mesi.

Comma 5
Chiunque, in violazione del divieto di cui all'articolo 187, effettua attività non consentite di miscelazione di rifiuti, è punito con la pena di cui al comma 1, lettera b).
Sanzione pecuniaria da centocinquanta a duecentocinquanta quote. La sanzione è ridotta della metà "nelle ipotesi di inosservanza delle prescrizioni contenute o richiamate nelle autorizzazioni, nonché nelle ipotesi di carenza dei requisiti e delle condizioni richiesti per le iscrizioni o comunicazioni." (D. Lgs. 152/06, art. 256, c. 4).

Comma 6, primo periodo
Chiunque effettua il deposito temporaneo presso il luogo di produzione di rifiuti sanitari pericolosi, con violazione delle disposizioni di cui all'articolo 227, comma 1, lettera b), è punito con la pena dell'arresto da tre mesi ad un anno o con la pena dell'ammenda da duemilaseicento euro a ventiseimila euro. Si applica la sanzione amministrativa pecuniaria da duemilaseicento euro a quindicimilacinquecento euro per i quantitativi non superiori a duecento litri o quantità equivalenti.
Sanzione pecuniaria fino a duecentocinquanta quote.

D. Lgs 152/06, art. 258 - Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari
Comma 4, secondo periodo
Le imprese che raccolgono e trasportano i propri rifiuti non pericolosi di cui all'articolo 212, comma 8, che non aderiscono, su base volontaria, al sistema di controllo della tracciabilità dei rifiuti (SISTRI) di cui all'articolo 188-bis, comma 2, lettera a), ed effettuano il trasporto di rifiuti senza il formulario di cui all'articolo 193 ovvero indicano nel formulario stesso dati incompleti o inesatti sono puniti con la sanzione amministrativa pecuniaria da milleseicento euro a novemilatrecento euro. Si applica la pena di cui all'articolo 483 del codice penale a chi, nella predisposizione di un certificato di analisi di rifiuti, fornisce false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti e a chi fa uso di un certificato falso durante il trasporto.
Sanzione pecuniaria da centocinquanta a duecentocinquanta quote.

D. Lgs 152/06, art. 260-bis - Sistema informatico di controllo della tracciabilità dei rifiuti
Comma 6
Si applica la pena di cui all'articolo 483 c.p. a colui che, nella predisposizione di un certificato di analisi di rifiuti, utilizzato nell'ambito del sistema di controllo della tracciabilità dei rifiuti fornisce false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti e a chi inserisce un certificato falso nei dati da fornire ai fini della tracciabilità dei rifiuti.
Sanzione pecuniaria da centocinquanta a duecentocinquanta quote.

Comma 7, secondo e terzo periodo
Il trasportatore che omette di accompagnare il trasporto dei rifiuti con la copia cartacea della scheda SISTRI - AREA MOVIMENTAZIONE e, ove necessario sulla base della normativa vigente, con la copia del certificato analitico che identifica le caratteristiche dei rifiuti è punito con la sanzione amministrativa pecuniaria da 1.600 euro a 9.300 euro. Si applica la pena di cui all'art. 483 del codice penale in caso di trasporto di rifiuti pericolosi. Tale ultima pena si applica anche a colui che, durante il trasporto fa uso di un certificato di analisi di rifiuti contenente false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti trasportati.

Sanzione pecuniaria da centocinquanta a duecentocinquanta quote.

Comma 8
Il trasportatore che accompagna il trasporto di rifiuti con una copia cartacea della scheda SISTRI - AREA Movimentazione fraudolentemente alterata è punito con la pena prevista dal combinato disposto degli articoli 477 e 482 del codice penale. La pena è aumentata fino ad un terzo nel caso di rifiuti pericolosi.
Sanzione pecuniaria da centocinquanta a duecentocinquanta quote (primo periodo) e da duecento a trecento quote (secondo periodo)

L. 549/93 Misure a tutela dell'ozono stratosferico e dell'ambiente
art. 3 - Cessazione e riduzione dell'impiego delle sostanze lesive Comma 6: Chiunque viola le disposizioni di cui al presente articolo è punito con l'arresto fino a due anni e con l'ammenda fino al triplo del valore delle sostanze utilizzate per fini produttivi, importate o commercializzate. Nei casi più gravi, alla condanna consegue la revoca dell'autorizzazione o della licenza in base alla quale viene svolta l'attività constituente illecito.
Sanzione pecuniaria da centocinquanta a duecentocinquanta quote.

In tema di rifiuti la responsabilità per l'attività di gestione non autorizzata non attiene necessariamente al profilo della consapevolezza e volontarietà della condotta, potendo scaturire anche da comportamenti che violino i doveri di diligenza per la mancata adozione di tutte le misure necessarie per evitare illeciti nella predetta gestione e che legittimamente si richiedono ai soggetti preposti alla direzione dell'azienda. Secondo i principi in materia di concorso di persone si può ritenere che il produttore di rifiuti nel momento in cui conferisce a un soggetto non autorizzato la gestione dei rifiuti, in quanto gravato da un obbligo di verifica della esistenza e regolarità dell'autorizzazione, risponde a titolo di concorso del reato di cui all'art. 256.

Ed ancora, ad avviso di costante giurisprudenza, il produttore/detentore di rifiuti speciali non pericolosi, qualora non provveda all'autosmaltimento o al conferimento dei rifiuti a soggetti che gestiscono il pubblico servizio, ha il dovere di accertarsi che coloro ai quali conferisce il rifiuto per il suo smaltimento definitivo siano forniti, ognuno per le attività di pertinenza (trasporto, stoccaggio provvisorio, smaltimento definitivo) delle necessarie autorizzazioni. L'omesso controllo sulla sussistenza di tale requisito comporta dunque una responsabilità penale quantomeno a titolo di colpa.

Da ultimo, si segnala che ad avviso della giurisprudenza ai fini della sussistenza del dolo specifico richiesto per l'integrazione del delitto di *attività organizzate per il traffico illecito di rifiuti* di cui all'art. 260, il profitto perseguito dall'autore della condotta può consistere anche nella semplice riduzione dei costi aziendali. Quest'ultima decisione assume una certa importanza anche ai fini dalla definizione di "interesse" e "vantaggio", che costituiscono i criteri di imputazione oggettiva previsti dall'art. 5 del d. lgs 231/2001 per estendere la responsabilità da reato all'ente.

4.2 DESTINATARI DELLA PARTE SPECIALE

I destinatari della parte speciale sono:
- Direzione;

- Legale e HR
- Amministrazione;
- Capo cantiere;
- i dipendenti;
- tutti coloro che a vario titolo lavorano per conto e con **ALTINTECH s.r.l.**

1.3 PRINCIPI DI COMPORTAMENTO

È vietato porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle qui considerate; sono altresì proibite le violazioni ai principi ed alle procedure aziendali previste nella presente Parte Speciale.

Fermo restando quanto sopra i Destinatari del presente Modello devono attenersi alle seguenti condotte:

- osservare rigorosamente tutte le leggi e i regolamenti e procedure in materia di ambiente che disciplinano lo svolgimento delle attività lavorative presso i locali aziendali e quelli in uso temporaneo;
- osservare le procedure e istruzioni di lavoro previste nel sistema di gestione ambientale ISO 14001
- partecipare ai corsi aziendali in materia di ambiente, ecologia e svolgimento delle specifiche mansioni, ai quali saranno invitati;
- segnalare alle funzioni competenti eventuali inefficienze dei mezzi e delle attrezzature, della documentazione a supporto.
- fornitori e gli altri Destinatari esterni alla **ALTINTECH s.r.l.** devono dare evidenza del rispetto da parte loro delle normative ambientali;

1.4 ATTIVITA' SPECIFICHE IN RIFERIMENTO ALLE OPERAZIONI A RISCHIO

Al fine di tutelare l'ambiente e ridurre gli impatti, sono previste specifiche procedure certificate da Ente terzo, secondo lo standard internazionale UNI EN ISO 14001.

- sono periodicamente individuati dal Datore di Lavoro gli impatti ambientali, tenendo in adeguata considerazione la struttura aziendale, la natura delle attività, l'ubicazione dei locali e delle aree di lavoro e l'organizzazione del personale. Nella valutazione degli impatti si adottano criteri oggettivi, documentati e ripetibili, considerando, per ognuno di essi, la probabilità di accadimento, la dimensione del danno possibile, i risultati di rilievi ambientali e la storia aziendale;

- i Destinatari del presente Modello sono tenuti a sorvegliare sull'effettivo rispetto delle procedure e sulla adozione delle adeguate misure di prevenzione, comunicando tempestivamente al Datore di Lavoro e/o all'OdV, eventuali eccezioni e criticità;

- alle ispezioni giudiziarie e amministrative devono partecipare i soggetti a ciò espressamente delegati. L'OdV dovrà essere prontamente informato sull'inizio di

ogni attività ispettiva e sull'evoluzione delle stesse. Copia dei verbali dell'ispezione devono essere conservati dall'OdV;

- sono previsti obblighi di riporto periodico all'OdV con riguardo a quanto previsto dal presente modello.

1.5 I CONTROLLI DELL'ODV

In merito a quanto disciplinato nella presente parte speciale, l'OdV ha i seguenti compiti:

- verificare periodicamente l'osservanza delle disposizioni del Testo unico ambientale e s.m.i. e delle procedure aziendali;

- analizzare le eventuali segnalazioni provenienti dai destinatari del Modello in merito al rispetto della normativa sulla sicurezza del lavoro.

SEZIONE II - PARTE SPECIALE G)

1. IMPIEGO DI CITTADINI DI PAESI TERZI IL CUI SOGGIORNO E' IRREGOLARE

1.1 TIPOLOGIE DI REATI

In considerazione delle attività oggi svolte dalla **ALTINTECH s.r.l.** si riporta la fattispecie rilevante**:** art. 22, comma 12-bis d. lgs. 25 luglio 1998, n. 286, introdotto tra i reati presupposto della responsabilità amministrativa degli enti con il d. lgs. 16 luglio 2012 n. 109.

In data 24 luglio 2012 è stato pubblicato sulla Gazzetta ufficiale il d. lgs 109/2012, con cui il legislatore ha inteso dare attuazione alla direttiva 2009/52/CE, contenente "norme *minime relative a sanzioni e provvedimenti nei confronti dei datori di lavoro che impiegano cittadini di paesi terzi il cui soggiorno è irregolare".*

Tra le principali novità, il legislatore ha introdotto nel decreto 231 l'art. 25- *duodecies* "Impiego *di cittadini terzi il cui soggiorno è irregolare",* che testualmente stabilisce: "in *relazione alla commissione del delitto di cui all'art. 22, comma 12-bis del decreto legislativo 25 luglio 1998, n. 286, si applica all'ente la sanzione pecuniaria da 100 a 200 quote, entro il limite dei 150.000 Euro".*

Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 22 d. lgs. 286/1998)12. *"Il datore di lavoro che occupa alle proprie dipendenze lavoratori stranieri privi del permesso di soggiorno previsto dal presente articolo, ovvero il cui permesso sia scaduto e del quale non sia stato chiesto, nei termini di legge, il rinnovo, revocato o annullato, è punito con la reclusione da sei mesi a tre anni e con la multa di 5.000 Euro per ogni lavoratore impiegato".*

La responsabilità amministrativa degli enti sussiste solo nelle ipotesi aggravate, disciplinate dal comma 12-bis, ossia quando:

- i lavoratori occupati sono in numero superiore a tre;

- i lavoratori occupati sono minori in età lavorativa;

- i lavoratori occupati sono sottoposti alle altre condizioni lavorative di particolare sfruttamento di cui al terzo comma dell'art. 603 bis del codice penale.

1.2 DESTINATARI DELLA PARTE SPECIALE

I destinatari della parte speciale sono:

- Direzione;
- Legale e HR
- Capocantiere;
- Tutti coloro che a vario titolo lavorano per conto e con **ALTINTECH s.r.l.**

Attività a rischio:

- gestione dei rapporti con il personale;
- gestione dei contratti di collaborazione professionale;
- gestione dei contratti di appalto e subappalto;
- gestione dei contratti con soggetti terzi (fornitori, consulenti ecc.).

1.3 PRINCIPI DI COMPORTAMENTO

E' vietato agli organi sociali, ai dipendenti, ai consulenti/Partner nella misura necessaria alle funzioni dagli stessi svolte di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, la fattispecie di reato in esame;
- violare i principi e le procedure esistenti in azienda in materia di assunzione del personale.

1.4 ATTIVITA' SPECIFICHE IN RIFERIMENTO ALLE OPERAZIONI A RISCHIO

Tutti i soggetti sopra indicati sono obbligati:

- a tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate all'assunzione di personale o, comunque, al suo impiego in Società;
- ad assicurare che il processo di assunzione sia condotto in maniera trasparente e documentabile e che sia basato su criteri non arbitrari e quanto possibile oggettivi, nel rispetto delle procedure aziendali interne e di quelle burocratiche vigenti, con particolare riguardo alle ipotesi di assunzione di lavoratori stranieri provenienti da paesi terzi,
- a considerare sempre prevalente la tutela dei lavoratori rispetto a qualsiasi valutazione economica;
- a verificare al momento dell'assunzione e durante lo svolgimento di tutto il rapporto lavorativo che eventuali lavoratori provenienti da paesi terzi siano in regola con il permesso di soggiorno e, in caso di scadenza dello stesso, abbiano provveduto a rinnovarlo;
- nel caso in cui si faccia ricorso al lavoro interinale mediante apposite agenzie, assicurarsi che tali soggetti si avvalgano di lavoratori in regola con la normativa di permesso di soggiorno e richiedere espressamente l'impegno a rispettare il modello;
- ad assicurarsi con apposite clausole contrattuali che eventuali soggetti terzi con cui la Società collabora (fornitori, consulenti etc.) si avvalgano di lavoratori in regola con la normativa in materia di permesso di soggiorno e richiedere espressamente l'impegno a rispettare il modello.
- i fornitori sono tenuti ad aderire formalmente al Codice di condotta per la fornitura di beni e l'esecuzione di prestazioni e/o servizi

Nello specifico è quindi fatto assoluto divieto di:

- assumere o comunque impiegare lavoratori stranieri privi di regolare permesso di soggiorno;
- assumere o comunque impiegare lavoratori stranieri il cui permesso di soggiorno sia scaduto e del quale non sia stato chiesto il rinnovo nei termini di legge;
- assumere o comunque impiegare lavoratori stranieri il cui permesso di soggiorno sia stato revocato o annullato.

Qualora la Società si avvalga di ditte appaltatrici per l'esecuzione di lavori dovrà chiedere direttamente all'appaltatrice documentazione finalizzata a comprovare la regolarità del lavoratore ivi operante. In tutti i contratti di appalto e subappalto per l'esecuzione di opere o lavori deve essere anche esplicitamente indicato, tra i vari obblighi a carico dell'appaltatrice/subappaltatrice o del somministratore, quello di verificare che ogni lavoratore proveniente da paesi terzi sia munito di regolare permesso di soggiorno in corso di validità.

1.5 I CONTROLLI DELL'ODV

In merito a quanto disciplinato nella presente parte speciale, l'OdV ha i seguenti compiti:

- verificare periodicamente l'osservanza delle disposizioni di legge e delle procedure aziendali;

- analizzare le eventuali segnalazioni provenienti dai destinatari del Modello in merito al rispetto della normativa del lavoro.

SEZIONE II - PARTE SPECIALE H)

1. SISTEMI “GENERALI” DI CONTROLLO

Le misure di prevenzione e di controllo “generali” contengono i presidi organizzativi generalmente idonei a ridurre l’esposizione a rischi di reato nella Società, e sono pertanto applicate da qualsiasi soggetto operante all’interno della medesima.

Tali misure di prevenzione e di controllo “generali” sono raggruppate nelle seguenti categorie:

1. Separazione delle funzioni incompatibili

2. Attribuzione delle deleghe in modo che vi sia piena corrispondenza tra le attività effettivamente svolte, i poteri esercitati o attribuiti, le procure conferite e le funzioni delegate

3. Procedimentalizzazione di ogni attività che comporti la formazione e attuazione delle decisioni della Società nelle aree sensibili

4. Flussi informativi periodici nei confronti del CdA e dell’OdV da parte delle Direzioni, dei Settori o Aree competenti, dedicati alle operazioni, in corso di esecuzione o concluse nel periodo di riferimento, che rientrano nelle attività sensibili

5. Analisi da parte del CdA e dell’OdV dei flussi informativi periodici provenienti dalle singole Funzioni aziendali competenti

6. Tracciabilità delle operazioni

7. Archiviazione dei documenti

8. Evidenza formale dei controlli

9. Misure di controllo relative alle attività svolte mediante strumenti informatici

10. Dovere di segnalazione da parte di ogni dipendente delle eventuali anomalie nella attuazione del Modello al Direttore o al Responsabile di Settore o Area

11.Dovere di fornire tempestiva informativa all’OdV di anomalie o violazioni del Modello Organizzativo da parte del Direttore o del Responsabile di Settore o di Area

12.Procedure relative alla gestione di ispezioni effettuate in azienda da pubbliche autorità ed enti pubblici

13. Previsione di clausole ad hoc che impongano il rispetto della *compliance* aziendale nei contratti con collaboratori esterni, consulenti, partner, fornitori

Viste le categorie delle misure di prevenzione e di controllo “generali”, si passa ora ad individuare le singole misure previste in ogni categoria:

Separazione delle funzioni incompatibili:

- l’autorizzazione di un’azione o di un atto è accordata da soggetto diverso da quello che compie l’azione o l’atto;
- il controllo interno sul compimento dell’azione o dell’atto è esercitato da soggetto ulteriormente diverso.

Attribuzione delle deleghe in modo che vi sia piena corrispondenza tra le attività effettivamente svolte, i poteri esercitati o attribuiti, le procure conferite e le funzioni delegate:

- il CdA adotta un sistema definito di responsabilità e deleghe che siano proporzionate alla conoscenza ed esperienza degli incaricati e in coerenza con le attività effettivamente da essi svolta;
- ciascun operatore deve curare che l’azione o atto che sta per compiere rientri tra quelli per cui egli è stato autorizzato in base alla procedura o alla delega;
- qualora venga compiuta un’azione o atto che, per competenza aziendale, spetterebbe a soggetto diverso, anche gerarchicamente di grado inferiore, devono essere documentate le ragioni con comunicazione al superiore gerarchico di chi li ha compiuti;

Procedimentalizzazione di ogni attività che comporti la formazione e attuazione delle decisioni della Società nelle aree sensibili:

- le attività emerse come sensibili sono disciplinate da procedure/protocolli, che diano completa attuazione dei principi di controllo di cui al presente e ai successivi paragrafi;

Flussi informativi periodici nei confronti del CdA e dell’OdV da parte delle Direzioni, dei Settori o Aree competenti, dedicati alle operazioni, in corso di esecuzione o concluse nel periodo di riferimento, che rientrano nelle attività a rischio:

- ogni Responsabile di Settore o Area o Funzione deve trasmettere tempestivamente al proprio Direttore la documentazione relativa alle operazioni connesse alle attività a rischio svolte nell’ambito del proprio Settore, Area o Unità secondo la mappatura indicata nella “Parte Speciale A-G” del presente Modello;
- ogni Direttore, Responsabile di Area o Settore, ovvero ogni singola Funzione o Unità, deve comunicare all’OdV eventuali segnalazioni relative al rischio concreto di commissione di “reati-presupposto” da parte di dipendenti;
- il Responsabile Legale/Risorse umane deve comunicare all’OdV la modifica dei poteri e delle attribuzioni conferite ai singoli dipendenti che ricoprano posizioni chiave nelle attività sensibili;
- il Dirigente preposto alla singola Direzione o il Responsabile dei Settori devono comunicare all’OdV la modifica delle procedure operative interne relative alle attività sensibili della propria Direzione o Settore;
- il Responsabile Legale/Risorse umane deve comunicare all’OdV ogni modifica della struttura o organigramma aziendale;

- il Dirigente preposto alla Direzione Amministrazione deve comunicare all'OdV ogni operazione societaria consistente, ad es., in fusione e scissione, cessione, acquisizione di azienda, etc.;
- il Responsabile della Contabilità (della Direzione Amministrazione) deve inviare al CdA e all'OdV rapporto riepilogativo su eventuali procedure relative alla richiesta di erogazioni pubbliche, ad operazioni straordinarie di tesoreria o finanziarie;
- il Responsabile Legale/Risorse umane deve inviare all'OdV informativa in relazione al mutamento dei soggetti preposti alle singole cariche direttive (Presidente, Amministratore Delegato, Direttori, Responsabili di Area o Settore, Funzione o Unità);
- il Responsabile della Settore Contabilità (della Direzione Amministrazione), prima della approvazione del progetto di bilancio deve inviare al CdA la bozza di bilancio. Successivamente all'approvazione del bilancio da parte del CdA, una copia del documento deve essere inviata all'OdV;

Analisi da parte del CdA e dell'OdV dei flussi informativi periodici provenienti dalle singole Funzioni aziendali competenti:

- l'OdV verifica i flussi informativi periodici provenienti dalle Direzioni, Settori o Aree analizzando il tipo di informazione pervenuta. Qualora dovessero emergere eventuali non conformità o attività a rischio reato, tenuto conto delle segnalazioni ricevute, l'OdV invia proposta al CdA per eventuale modifica del Modello Organizzativo;
- l'OdV propone, in ordine alle conseguenze delle non conformità rilevate, le contestazioni da promuovere nei confronti dei soggetti inadempienti;
- l'OdV formula proposte al CdA per aggiornamenti e adeguamenti del Modello Organizzativo;

Tracciabilità delle operazioni:

- i sistemi informatici aziendali devono garantire la tracciabilità dei singoli passaggi e l'identificazione dell'operatore dal quale viene inserito o modificato il dato nel sistema;
- il Direttore o Responsabile di ciascuna Area o Settore, ovvero ogni singola Funzione o Unità coinvolta nel processo, deve curare la tracciabilità delle informazioni non generate in automatico dal sistema informatico tramite adeguata documentazione cartacea che deve essere accuratamente archiviata;
- i soggetti che intervengono nello svolgimento delle predette attività si accertano che vengano effettuati salvataggi (back–up) periodici dei dati (ad es. dati contabili o aziendali);
- i dati presenti nel sistema informatico possono essere cancellati ad opera del soggetto che li aveva generati solo in via eccezionale, previa autorizzazione scritta e motivata del proprio superiore gerarchico, con documentazione evidenziante il dato cancellato debitamente archiviata. Resta fermo che il sistema deve essere in grado di registrare l'avvenuto intervento di cancellazione;

Archiviazione dei documenti:

- ciascun operatore deve curare che ogni operazione che svolge sia tempestivamente documentata;
- ciascun operatore deve curare la tempestiva archiviazione della documentazione di

ogni operazione svolta;
- ciascun operatore deve custodire la documentazione archiviata;
- l'accesso alla documentazione archiviata è consentito agli organi di controllo aziendali (OdV) o dietro autorizzazione scritta del soggetto sovraordinato;

Evidenza formale dei controlli:
- i controlli che vengono effettuati all'interno di un processo devono lasciare una traccia documentale, così che si possa, anche in un momento successivo, verificare lo svolgimento del controllo, identificare colui che lo ha posto in essere e valutarne l'operato;

Misure di controllo relative alle attività svolte mediante strumenti informatici:
- ogni PC in uso presso la Società richiede codici di accesso;
- ogni PC è assegnato ad un solo utente che vi accede mediante propri dati identificativi;
- le richieste per l'attribuzione di codici di accesso alla rete aziendale sono inoltrate al servizio competente (IT) da soggetto diverso dal beneficiario dell'autorizzazione ma in relazione funzionale con questo;
- la richiesta di autorizzazione all'accesso per gli esterni (es. consulenti) vengono inoltrate dal soggetto titolare o responsabile in ALTINTECH del rapporto con l'esterno medesimo;
- i dati per l'accesso a ciascun PC della Società devono esser rilasciati dal Responsabile IT solo su autorizzazione da parte di un Dirigente;
- le richieste di rimozione dell'accesso o modifica dei propri dati identificativi devono pervenire al Responsabile IT da parte dello stesso utente personalmente o a mezzo di un delegato ovvero dal suo diretto responsabile;
- chi apre cartelle condivise o vi effettua comunque operazioni è considerato responsabile della cartella condivisa;
- sono adottate misure di sicurezza per evitare l'accesso, da parte di esterni, alla rete di accesso ad internet e per garantire la sicurezza e la riservatezza delle informazioni e dei dati inseriti nella rete aziendale;
- eventuali comunicazioni telematiche alla Pubblica Amministrazione devono essere effettuate esclusivamente dal Direttore o Responsabile competente ovvero con sua preventiva autorizzazione scritta;
- tutte le regole e le procedure in tema di uso degli strumenti informatici o telematici integrano quelle standard;
- tutti i cambiamenti, modifiche, cancellature riguardanti i master file di ciascun cliente devono essere gestiti in maniera completa, corretta e tempestiva;
- tutti i clienti ricollegabili ad enti governativi sono contraddistinti con apposita evidenziazione;
- il Responsabile IT definisce ed approva metodi per il controllo dell'accesso al sistema al fine di evitare rischi di accesso non abilitato ai sistemi informatici ed assicurando la corretta applicazione di quanto previsto dal Regolamento UE 679/16

Dovere di segnalazione da parte di ogni dipendente delle eventuali anomalie al Direttore o
al Responsabile di Settore o Area:
- chi riscontri eventuali anomalie le comunica per iscritto al proprio superiore, in modo

da assicurare la tracciabilità e verificabilità del rilievo;
- chi riceve la comunicazione dell'anomalia deve effettuare azione correttiva per eliminarla e tale operazione deve essere documentata:

Dovere di fornire tempestiva informativa all'OdV di anomalie o violazioni del Modello Organizzativo da parte dei Direttori e dei Responsabili di Settore o Area:
- ogni dipendente e chiunque operi a nome o nell'interesse della Società è tenuto a comunicare per iscritto e in modo tempestivo all'Organismo di Vigilanza la notizia circa comportamenti anomali, anche se non ancora di rilevanza penale, tenuti in ambito aziendale, ovvero qualsiasi violazione del Modello Organizzativo di cui sia venuto a conoscenza;

Procedure relative alla gestione di ispezioni effettuate in azienda da pubbliche autorità ed enti pubblici:
- in caso di ispezione, visita, verifica richiesta di documentazione o informazioni da parte di autorità o enti quali (in via esemplificativa: agenzia delle entrate, enti previdenziali, Guardia di Finanza, ASL, Carabinieri, etc.), il soggetto che riceve avviso di tali ispezioni, visite, verifiche, richieste di documentazione o informazioni ne dà immediata comunicazione all'Amministratore Delegato, alla Direzione Amministrazione e all'OdV;

Previsione di clausole ad hoc che impongono il rispetto della compliance aziendale nei contratti con collaboratori esterni, consulenti, partner, fornitori:
- nei contratti stipulati con collaboratori esterni, consulenti, partner e fornitori devono essere inserite specifiche clausole con cui gli stessi attestino di essere a conoscenza del Modello Organizzativo e si impegnino a uniformarsi ai principi e alle procedure in essi contenuti
- i contratti devono prevedere che comportamenti violativi dell'obbligo così assunto consentano la risoluzione del contratto (clausola risolutiva espressa, penale, ecc.);
- ai collaboratori esterni, ai consulenti e ai fornitori che intrattengono rapporti con la P.A. per conto della Società, deve esser formalmente conferito potere in tal senso (con apposita clausola inserita nel contratto);
- gli stessi soggetti devono sottoscrivere una dichiarazione in cui si attesta la conoscenza del Modello Organizzativo e l'impegno di uniformarsi ai principi e alle procedure in essi contenuti.

La società si è dotata di procedure interne che si ispirano ai principi riportati sopra:

- Procedura Apertura Impegno
- Procedura Superamento Budget
- Procedura Sanzioni Disciplinari
- Procedura linee guida per la comunicazione in azienda
- Procedura Arrivo Ordini e Richiesta Assegnazione PM
- Procedura Gestione Apertura Cantiere
- Procedura Gestione Trasferte
- Procedura Utilizzo e Cura dei Mezzi Aziendali
- Procedura Permessi_Ferie_STD

- Procedura Acquisto Materiali
- Procedura Offerte e Marginalità da applicare
- Procedura Registrazione Beni ed assegnazione

SEZIONE II - PARTE SPECIALE I)

1. PROCEDURA DEL SISTEMA DI CONTROLLO DI GESTIONE

i. SCOPO E CAMPO DI APPLICAZIONE

La presente procedura definisce compiti, responsabilità, autorità e modalità operative per la pianificazione e l'effettuazione degli Audit da parte dell'OdV. La presente procedura si applica a tutto il personale coinvolto.

ii. RIFERIMENTI NORMATIVI

D. Lgs. 231/01 e s.m.i.

iii. DEFINIZIONI

Le definizioni dei termini utilizzati nella presente procedura sono contenute nel D. Lgs. 231/01 e s.m.i., nel Modello di Organizzazione, Gestione e Controllo preventivo, nello standard UNI EN ISO 19011:2012.

iv. DESCRIZIONE DEL PROCESSO

Gli Audit previsti nel Modello sono uno strumento aziendale per: valutare la capacità di prevenzione del Modello organizzativo (adeguatezza), controllare i processi di mappatura delle aree a rischio e dei segnali premonitori di potenziali irregolarità (risk assessment), vigilare sull'effettiva applicazione del modello, effettuare analisi di compliance al Modello, proporre gli aggiornamenti al Modello organizzativo.

I verbali di Audit devono dare evidenza oggettiva della necessità di ridurre, eliminare e, soprattutto, prevenire eventuali non conformità.

Gli Audit sono:

- programmati dall'OdV, opportunamente pianificati ed effettuati annualmente;
- svolti a sorpresa o su segnalazione o ad hoc, per verificare l'efficacia di una azione correttiva/preventiva adottata in merito ad una non conformità emersa o in seguito ad interventi di miglioramento.

Gli Audit vengono condotti secondo lo standard UNI EN ISO 19011:2012 tramite interviste al personale responsabile supportate dai riscontri documentali delle registrazioni effettuate nell'esecuzione dell'attività stessa.

v. RUOLI E RESPONSABILITÀ

La responsabilità dell'attività delle verifiche ispettive interne della qualità spetta al Presidente dell'OdV. Gli Audit sono svolti dai membri dell'OdV. Quando l'OdV lo ritiene opportuno può avvalersi della collaborazione aggiuntiva di un altro valutatore qualificato; in questo caso si forma un gruppo di verifica di cui il Presidente dell'OdV è sempre e comunque responsabile.

In particolare il Responsabile del gruppo di verifica deve:

- predisporre il "Piano dell'Audit";
- esaminare la documentazione relativa alle attività per valutarne la adeguatezza;
- registrare qualsiasi ostacolo rilevante incontrato nel corso della verifica;
- verbalizzare i risultati della verifica in modo chiaro;
- comunicare immediatamente le risultanze al Presidente.

Nell'effettuare l'Audit è necessario:

- rimanere entro i limiti previsti;
- agire con obiettività e nei limiti di quanto previsto dalla mission;
- essere in grado di valutare se: 1) le procedure che descrivono ed i documenti che registrano e supportano gli elementi richiesti dal Modello organizzativo sono conosciuti, disponibili, compresi ed utilizzati dal personale della Funzione Aziendale oggetto di valutazione; 2) i documenti e le altre informazioni usati per descrivere il Modello organizzativo sono tutti adeguati per conseguire gli obiettivi di riduzione del rischio stabiliti.

Il Responsabile della Funzione Aziendale oggetto di Audit deve:

- assistere all'esecuzione della verifica ispettiva;
- fornire gli elementi di oggettiva evidenza secondo quanto richiesto dal Responsabile, collaborando con essi al raggiungimento degli obiettivi della verifica;
- definire ed avviare azioni correttive basate sul rapporto di Audit.

vi. DOCUMENTAZIONE DI LAVORO

I documenti relativi all'esecuzione degli Audit sono:

1) Piano di Audit

Il piano della funge da documento di convocazione della riunione o da comunicazione dell'attività da svolgere. Una volta approvato, il piano annuale viene trasmesso per conoscenza al Presidente, entro il mese di gennaio di ciascun anno solare, mediante comunicazione interna.

2) Rapporto di Audit

Questo documento deve contenere:
- identificazione della/e Funzioni Aziendali;
- identificazione dei Responsabili della/e Funzioni Aziendali;
- identificazione di altri collaboratori intervistati;
- obiettivi (area) ed estensione della verifica (parti dell'area);
- identificazione dei documenti di riferimento;

- data dell’Audit;
- identificazione dei componenti del gruppo di verifica;
- data e firma del Presidente dell’OdV.

Il Rapporto deve riportare fedelmente i contenuti delle risultanze e contiene la menzione delle anomalie riscontrate nel corso dell’ Audit. Esso deve essere datato e firmato dai membri del team di Audit.

Il Rapporto è composto:
- da una copertina (primo foglio);
- pagine successive per le risultanze.

La copertina deve essere compilata indicando:
- il numero progressivo del rapporto;
- data;
- numerazione delle pagine;
- documenti di riferimento;
- indicazione dello scopo della verifica

Nelle pagine interne è indicata la classificazione delle anomalie.

vii. ESECUZIONE DELL’AUDIT

Le evidenze devono essere raccolte mediante:
- interviste;
- esame dei documenti;
- osservazione delle attività nelle area di interesse secondo quanto descritto nel Modello.

Quando possibile, il team deve verificare le informazioni ricevute e le registrazioni controllate, acquisendo le stesse informazioni da altre fonti indipendenti dalla Funzione Aziendale oggetto di verifica.

Le indicazioni di "non conformità" o "osservazioni" devono essere annotate se appaiono anomalie significative.
Ai fini dell'attribuzione, di seguito sono riportate le definizioni delle anomalie:

- NON CONFORMITA' = Parziale o totale non compliance al Modello organizzativo
- OSSERVAZIONI = Errata applicazione di una o più parti del Modello organizzativo

I membri dell’OdV hanno la responsabilità di definire, concordare con P ed intraprendere le azioni correttive/preventive necessarie per risolvere le anomalie emerse, rimuovendo le cause.
Le azioni correttive/preventive e la successiva verifica della loro attuazione devono essere completate entro un periodo di tempo stabilito e concordato tra il Responsabile della Funzione Aziendale ed il Responsabile del gruppo di Audit.

Il Responsabile del gruppo di verifica deve tenere informato P e il Responsabile sullo stato di attuazione delle azioni correttive/preventive e sulle successive verifiche.
Dopo aver accertato l'attuazione delle azioni correttive/preventive, il gruppo di Audit opera secondo le medesime modalità seguite per la verifica originale.

viii. DOCUMENTAZIONE

- Piano annuale di Audit
- Rapporto di Audit

I rapporti, unitamente ai piani annuali, sono conservati a cura dell'OdV presso l'Archivio Aziendale.

2. PROCEDURA WHISTLEBLOWING PER LE SEGNALAZIONI DI ILLECITI E IRREGOLARITÀ

i. SCOPO E CAMPO DI APPLICAZIONE

La presente procedura disciplina le modalità di segnalazione degli illeciti cd. "Whistleblowing" (in inglese soffiata nel fischietto) nell'ambito delle attività di prevenzione della corruzione, come descritto nel sistema ISO 37001 certificato e nel Codice Etico.

Scopo della procedura è di rimuovere i fattori che possono ostacolare o disincentivare la segnalazione, come ad esempio i dubbi sulla procedura da seguire e i timori di ritorsioni o discriminazioni.
A tale fine la procedura ha l'obiettivo di fornire al whistleblower le indicazioni operative su come effettuare la segnalazione.

ii. RIFERIMENTI NORMATIVI

- D.lgs. n. 24/2023
- Reg. UE 679/15 GDPR

iii. DEFINIZIONI

Con l'espressione whistleblower si fa riferimento al portatore di interesse che rileva una possibile frode, un pericolo o un altro rischio che possa danneggiare lavoratori, azionisti, fornitori, soci, il pubblico o la stessa reputazione della società e la segnala agli organi legittimati a intervenire (Organismo di Vigilanza e Responsabile per la prevenzione della corruzione e trasparenza in ALTINTECH riuniti nella stessa persona).

iv. RESPONSABILITA'

L'Organismo di Vigilanza e Responsabile per la prevenzione della corruzione e trasparenza ha le seguenti responsabilità relativamente al Whistleblowing:

- inviare una notifica di ricezione della comunicazione al whistleblower, entro i termini previsti dalla legge.
- rispondere agli atti dell'inchiesta.
- mantenere sempre la riservatezza sull'informatore, anche nei confronti degli organi direttivi dell'azienda.
- mantenere la comunicazione con l'informatore nel caso in cui siano necessarie ulteriori informazioni sui fatti denunciati.
- informare il whistleblower dei suoi diritti e delle azioni che può intraprendere per tutelarsi all'interno dell'azienda.
- mantenere sempre il rispetto della presunzione di innocenza e dell'onore delle persone coinvolte.
- trasmettere immediatamente tutte le informazioni pertinenti alla Procura della Repubblica quando i fatti potrebbero essere indicativi di un'accusa penale. Se i fatti riguardano gli interessi finanziari dell'Unione europea, la questione deve essere deferita alla Procura europea.

v. DESCRIZIONE DEL PROCESSO

Le fasi della procedura interna sono le seguenti:

1. fase dell'iniziativa
2. fase dell'istruttoria
3. fase della decisione

1. Fase dell'iniziativa

I canali per la trasmissione della segnalazione sono:

a) l'applicazione informatica Monday.com nel modulo appositamente sviluppato;
b) la casella di posta elettronica istituzionale dell'OdV/RPCT odv@altintech.it;
c) il servizio postale (posta ordinaria o con raccomandata con ricevuta di ritorno e indirizzate al RPCT con la dicitura riservata personale);
d) consegna brevi manu in sede (ovvero in busta chiusa indirizzata all'OdV/RPCT RPCT con la dicitura riservata personale).

Nel primo caso il segnalante si accredita su una applicazione informatica accessibile agli utenti interni ed esterni, nella quale è sviluppato l'applicativo di gestione delle segnalazioni.
L'applicazione è accessibile:

- attraverso il link della intranet aziendale;
- da qualsiasi dispositivo mobile attraverso il link nell'home page di www.altintech.it

L'applicazione consente di compilare, inviare e ricevere in modo informatizzato il "Modulo di segnalazione".
A seguito dell'inoltro della segnalazione, l'autore riceve dal sistema un codice identificativo utile per i successivi accessi.
I dati della segnalazione (unitamente agli eventuali documenti allegati) vengono automaticamente inoltrati all'OdV/ RPCT.

Le segnalazioni inoltrate con le modalità sopra elencate vengono protocollate in modalità riservata e salvate, insieme ai successivi atti connessi, in una cartella informatica riservata consultabile dall'OdV/RPCT.
Qualora la segnalazione sia stata presentata brevi manu, la stessa sarà costudita, insieme a tutta la documentazione pervenuta, in un armadio chiuso a chiave nella stanza del RPCT, avendo cura di separare i dati identificativi del segnalante dalla restante documentazione, la quale sarà eventualmente affidata al funzionario deputato agli approfondimenti istruttori.

2. Fase dell'istruttoria

Entro 5 giorni lavorativi, l'OdV/RPCT invia al segnalante un avviso di ricevimento e prende in carico la segnalazione per una prima sommaria istruttoria da effettuare entro altri 5 giorni dalla data di trasmissione dell'avviso.

L'OdV/RPCT analizza la segnalazione al fine di determinarne l'ammissibilità e la ricevibilità e, se quanto denunciato non è stato adeguatamente circostanziato, richiede chiarimenti al segnalante mediante l'applicativo informatico. Nel caso di segnalazione recapitata secondo altre modalità, il responsabile dell'istruttoria richiede approfondimenti attraverso mail, se nota, protocollata in modalità riservata.

Possono a questo punto verificarsi due situazioni:

i. Archiviazione.

Nel caso in cui si rilevi un'evidente e manifesta infondatezza, inammissibilità o irricevibilità si procede ad archiviare la segnalazione. Nello specifico, costituiscono possibili causali di archiviazione:

- manifesta mancanza di interesse all'integrità aziendale.
- manifesta incompetenza dell'OdV/RPCT sulle questioni segnalate.
- contenuto generico della segnalazione/comunicazione o tale da non consentire nessun approfondimento.
- segnalazioni aventi ad oggetto i medesimi fatti trattati in procedimenti già definiti.

Se procede all'archiviazione, l'OdV/RPCT valuterà se la segnalazione (e la relativa documentazione) debba essere trasmessa ad altri uffici interni per competenza.

ii. Approfondimento e verifica.

Nell'ipotesi in cui non ricorra alcuno dei casi di archiviazione sopra riportati, l'OdV/RPCT provvede a verificare la segnalazione ricevuta, anche acquisendo ogni elemento utile alla valutazione della fattispecie, avendo cura di adottare misure idonee ad assicurare la riservatezza dell'identità del segnalante laddove gli approfondimenti richiedano il necessario coinvolgimento di soggetti terzi.
Ciò anche attraverso:

- richiesta di notizie, informazioni, atti e documenti al dirigente responsabile del processo interessato.
- richiesta di notizie, informazioni, atti e documenti al CdA
- richiesta di chiarimenti, documentazione e informazioni ulteriori al segnalante (mediante il sistema informatico o attraverso mail se nota) e/o a eventuali altri soggetti terzi coinvolti nella segnalazione
- audizione del Whistleblower.

Successivamente procede all'analisi della documentazione e degli elementi ricevuti e a deliberare sul fumus di quanto rappresentato nella segnalazione (ciò in quanto il l'OdV/RPCT non accerta i fatti, ma svolge un'attività di verifica e di analisi).

L'OdV/RPCT dovrà verificare:

a) se quelle segnalate sono "condotte illecite";
b) se le suddette condotte riguardano, o meno, situazioni di cui il soggetto è venuto direttamente a conoscenza 'in ragione del rapporto di lavoro';
c) se si tratta di notizie acquisite in occasione e/o a causa dello svolgimento delle mansioni lavorative, seppure in modo casuale, anche nelle fasi preliminari all'instaurazione del rapporto di lavoro o prima del suo termine.
d) se la segnalazione è stata inoltrata "nell'interesse dell'integrità aziendale";

Saranno archiviate le doglianze di carattere personale del segnalante o rivendicazioni/istanze che attengono alla disciplina del rapporto di lavoro o rapporti con superiori gerarchici e colleghi in quanto non rientranti nell'ambito di applicazione della norma.

Non saranno prese in considerazione le segnalazioni fondate su meri sospetti o voci: risulta necessario, infatti, sia tenere conto dell'interesse dei terzi oggetto delle informazioni riportate nella segnalazione, sia evitare che l'azienda promuova attività ispettive interne che rischiano di essere poco utili e, comunque, dispendiose.

3. Fase decisoria

Qualora venga rilevata una delle cause di archiviazione sopra elencate, entro e non oltre 30 giorni dall'invio dell'avviso di ricevimento il OdV/RPCT provvede a:

a) archiviare la segnalazione con adeguata motivazione. La stessa verrà, quindi, inserita e conservata all'interno dell'applicazione aziendale;
b) comunicare al segnalante l'archiviazione e la relativa motivazione mediante il sistema informatico (o altro canale utilizzato per la segnalazione).

In caso, invece, di accertamento della fondatezza della segnalazione, il OdV/RPCT provvede a redigere una relazione contenente le risultanze dell'istruttoria condotta ed i profili di illiceità riscontrati nonché a:

a) inviare la summenzionata relazione e l'eventuale documentazione e omettendo l'indicazione dell'identità del segnalante, al CdA per l'avvio del procedimento disciplinare (se si tratta di un'ipotesi di illecito disciplinare);
b) comunicare al segnalante l'inoltro della segnalazione alle Autorità e la relativa motivazione e ad avvisarlo della eventualità che la sua identità potrà essere fornita all'Autorità giudiziaria.

Per garantire la gestione e la tracciabilità delle attività svolte, l'OdV/RPCT assicura la conservazione all'interno del sistema delle segnalazioni e di tutta la correlata documentazione di supporto per un periodo di cinque anni dalla ricezione, assicurando che i dati identificativi del segnalante siano conservati separatamente da ogni altro dato.

vi. SOGGETTI COMPETENTI A GESTIRE LE SEGNALAZIONI

L'OdV/RPCT è per legge il soggetto deputato a dare seguito alle segnalazioni.
Qualora le segnalazioni riguardino una condotta tenuta dal RPCT, quest'ultimo si trova in posizione di conflitto di interessi. Appare, pertanto, opportuno che dette ipotesi siano trattate dal CdA in quanto organo sovraordinato.

vii. TUTELA DELLA RISERVATEZZA E DIRITTO DI ACCESSO

Tutta la procedura mira ad assicurare la separazione tra i contenuti della segnalazione e gli elementi che consentono di risalire all'identità del whistleblower.
Al fine di garantire la massima tutela della riservatezza, l'accesso alla documentazione è consentito al solo OdV/RPCT.

L'utilizzo della applicazione informatica, inoltre, agevola l'espletamento degli accertamenti da parte degli istruttori, consentendo loro l'interlocuzione diretta con il segnalante senza la necessità che sia acquisito il suo nominativo.

Laddove, invece, la segnalazione sia stata trasmessa con un canale diverso dal sistema informatico a ciò deputato, l'OdV/RPCT avrà cura di oscurare gli elementi informativi che

consentano l'identificazione del segnalante, se l'informazione deve essere condivisa con altri, e provvedendo direttamente alle interlocuzioni, ove necessarie.
Nell'ipotesi in cui non risulti materialmente possibile assicurare tale livello di riservatezza, la segnalazione sarà trattata direttamente da OdV/RPCT.

Quest'ultimo, inoltre, è l'unico soggetto che possiede tutte le informazioni necessarie e utili per apprezzare correttamente se effettivamente sussistono i presupposti normativamente previsti per svelare l'identità del segnalante. In particolare, qualora la richiesta di conoscere l'identità del segnalante pervenga dall'Autorità giudiziaria o contabile l'OdV/RPCT controllerà la ricorrenza, o meno, degli elementi minimi previsti dalla legge (ovvero l'instaurazione di un procedimento penale o contabile).

Diversamente, nel caso in cui l'OdV/RPCT trasmetta gli atti al CdA per i procedimenti disciplinari, la discovery è subordinata ad una specifica richiesta del secondo il quale rappresenti che la conoscenza dell'identità del segnalante è indispensabile per la difesa dell'incolpato.
In tal caso l'OdV/RPCT, dopo aver verificato che la contestazione risulta fondata, in tutto o in parte, sulla segnalazione, provvederà ad acquisire, attraverso la applicazione informatica o altro canale con il quale è stata inviata la comunicazione, il consenso del segnalante a rivelare l'identità mediante una dichiarazione sottoscritta da quest'ultimo (a cui dovrà essere allegato idoneo documento attestante l'identità del dichiarante).

Il divieto di rilevare l'identità del segnalante è da riferirsi non solo al nominativo del segnalante, ma anche a tutti gli elementi della segnalazione, inclusa la documentazione ad essa allegata, nella misura in cui il loro disvelamento, anche indirettamente, possa consentire l'identificazione del segnalante. Il trattamento di tali elementi va, quindi, improntato alla massima cautela, a cominciare dall'oscuramento dei dati qualora per ragioni istruttorie altri soggetti ne debbano essere messi a conoscenza.

viii. MODALITA' DI GESTIONE DELLE SEGNALAZIONI

Modalità di conservazione dei dati (fisico, logico, ibrido)	Le modalità si differenziano a seconda che la segnalazione, e la correlata documentazione, sia pervenuta: • tramite sistema informatico (piattaforma o protocollo): logico • con modalità cartacea o via mail: ibrido
Politiche di tutela della riservatezza attraverso strumenti informatici (disaccoppiamento dei dati del segnalante rispetto alle informazioni relative alla segnalazione, crittografia dei dati e dei documenti allegati)	Nel caso di gestione del procedimento attraverso il sistema informatico: • la piattaforma utilizza un protocollo di crittografia SHA 256 che garantisce una tutela rafforzata della riservatezza dell'identità del segnalante, del contenuto della segnalazione e della documentazione ivi allegata. Attraverso il suddetto protocollo di crittografia i dati identificativi del dipendente vengono segregati in una Sezione dedicata della piattaforma, accessibile solo all'OdV/RPCT. Nel caso di segnalazione pervenuta attraverso un'altra modalità:

	• la segnalazione e la documentazione pervenuta brevi manu è custodita in un armadio chiuso, mentre quella inviata a mezzo protocollo informatico o per posta elettronica, certificata e no, è protocollata e archiviata all'interno del protocollo informatico con modalità riservata.
Politiche di accesso ai dati	Applicazione informatica: I dati relativi alle condotte illecite segnalate sono contenuti, insieme alla documentazione allegata, in un data base, al quale può accedere soltanto il personale autenticato. In prima battuta solo l'OdV/RPCT, può visualizzare l'elenco delle segnalazioni e delle comunicazioni acquisite dal sistema non ancora esaminate ed assegna la pratica. Inoltre, l'OdV/RPCT è l'unico soggetto che conosce l'identità del segnalante. L'amministratore del sistema informatico, invece, è responsabile tecnico dell'applicazione e non accede ai dati del segnalante né alle pratiche presenti nel sistema. Segnalazione pervenuta brevi manu/via mail: I dati relativi alle condotte illecite segnalate sono contenuti, insieme alla documentazione allegata, all'interno di uno specifico fascicolo riservato al quale può accedere soltanto l'OdV/RPCT.
Politiche di sicurezza. Modifica periodica delle password.	La password verrà modificata ogni 6 mesi come da prescrizioni del protocollo GDPR.
Tempo di conservazione dei dati e documenti	5 anni.
Tempistica di svolgimento del procedimento	Termini: • 05 giorni per l'invio dell'avviso di ricevimento; • 05 giorni lavorativi per l'esame preliminare della segnalazione cui consegue l'avvio dell'istruttoria (decorre dalla data di invio dell'avviso); • 10 giorni per la definizione dell'istruttoria che decorrono dalla data di avvio della stessa.
Responsabilità relative alla sicurezza informatica delle informazioni	Amministratore del sistema.
Responsabilità relative al trattamento dei dati	Nel corso del procedimento titolare del trattamento dei dati (come definito dall'art. 4, Regolamento UE 2016/679) è l'OdV/RPCT.

	Nell’ipotesi di richiesta di conoscere il nominativo del segnalante, è l’Autorità giudiziaria o contabile richiedente dal momento in cui riceve il dato.