INFORMATICA TRENTINA SpA

Modello Organizzativo, di gestione e controllo ex D.Lgs. 231/2001

Approvato dal Consiglio di Amministrazione con delibera del 19/06/2018

PRINCIPALI MODIFICHE RISPETTO ALLA VERSIONE PRECEDENTE

Data	Versione	Modifiche apportate
06/07/2009	01.0 Obsoleto	Prima stesura
29/03/2010	01.1 Obsoleto	Aggiornamento a seguito aggiunta nel D.Lgs. 231/2001 di nuove categorie di reato e correzione terzo punto elenco al par. 6.1
22/12/2010	01.2 Obsoleto	Aggiornamento a seguito dell'assegnazione dei nuovi poteri e deleghe di amministrazione e rappresentanza (par. 5.4)
12/12/2011	01.3 Obsoleto	Aggiornamento par. 2.1 a seguito aggiunta nel D.Lgs. 231/2001 di nuove categorie di reato (reati ambientali)
06/12/2012	01.4 Obsoleto	Aggiornamento par. 2.1 a seguito aggiunta nel D.Lgs. 231/2001 di nuove categorie di reato (Impiego di cittadini di paesi terzi il cui soggiorno è irregolare), par. 5.3 per migliorare descrizione dei controlli e par. 5.4 a seguito dell'assegnazione dei nuovi poteri e deleghe di amministrazione e rappresentanza
20/06/2013	01.5 Obsoleto	Aggiornamento par. 5.4 a seguito dell'assegnazione di nuovi poteri e deleghe di amministrazione e rappresentanza (delibera CdA del 15 novembre 2012)
13/01/2014	01.6 Obsoleto	Aggiornamenti diffusi per recepire gli adempimenti connessi alla Legge n. 190/2012 previsti per gli enti di diritto privato in controllo pubblico
15/11/2016	01.7 Obsoleto	Aggiornamenti diffusi per recepire l'attribuzione al Responsabile della prevenzione della corruzione e della trasparenza i compiti previsti Legge n. 190/2012, nonché integrazioni al par. 6 a seguito della revisione dei contenuti del Regolamento dell'Organismo di Vigilanza
19/06/2018	01.8 In vigore	Aggiornamenti al par. 2.1 per recepire aggiunta nel D.Lgs. 231/2001 di nuove categorie di reato (Razzismo e xenofobia), al par. 7.1.1 per le integrazioni al sistema disciplinare con le misure per gli Amministratori e al par. 6.5 per la tutela degli autori di segnalazioni di reati o irregolarità

Le variazioni apportate rispetto alla precedente versione sono evidenziate mediante barra verticale sul margine destro.

INDICE

1 INTRODUZIONE

1.1 PREMESSA

Il presente documento descrive il Modello di organizzazione, gestione e controllo ex D.Lgs. n. 231/2001 adottato da Informatica Trentina S.p.A. volto a prevenire la realizzazione dei reati espressamente previsti dal Decreto, integrato con le misure per la prevenzione della corruzione ai sensi della Legge 6 novembre 2012, n.190 "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione".

Il documento è articolato nei seguenti capitoli:

1) la normativa di riferimento, che riporta in sintesi la struttura e gli elementi ritenuti fondamentali per l'adeguamento al Decreto e alla Legge n. 190/2012;
2) la metodologia seguita per l'individuazione delle attività sensibili;
3) il Modello 231, che descrive l'impostazione del Modello di organizzazione, gestione e controllo adottato dalla Società;
4) il sistema organizzativo, che descrive la documentazione inerente i processi organizzativi adottati dalla Società;
5) l'Organismo di Vigilanza, che indica le linee guida che detto organismo deve tenere al fine di verificare la tenuta ed la corretta manutenzione del Modello di organizzazione, gestione e controllo;
6) il sistema disciplinare;
7) le linee di condotta 231, che cita le linee di comportamento da tenere nei rapporti con i diversi interlocutori della Società;
8) la formazione, la diffusione, il riesame e l'aggiornamento del Modello 231.

1.2 GLOSSARIO

Attività sensibile: processo/attività nel cui ambito ricorre il rischio di commissione dei reati contemplati dal Decreto e dalla L. 190/2012; trattasi dei processi nelle cui fasi, sottofasi o attività si potrebbero in linea di principio configurare le condizioni, le occasioni o i mezzi per la commissione di reati contemplati dal Decreto e dalla L. 190/2012 anche in concorso con altri Enti

Autorità: Autorità Giudiziaria, Istituzioni e Pubbliche Amministrazioni locali, nazionali ed estere, Consob, Banca d'Italia, Antitrust, Borsa Italiana, "Garante della privacy" e altre Autorità di vigilanza italiane ed estere

C.d.A.: Consiglio di Amministrazione

CCNL: Contratto Collettivo Nazionale di Lavoro

D.Lgs. 231/2001 o **Decreto**: il Decreto Legislativo dell'8 giugno 2001 n. 231, recante «Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300», e successive modifiche ed integrazioni

L. 190/2012: la Legge 6 novembre 2012, n.190 recante "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione", e successive modifiche e integrazioni

Modello 231: il Modello di organizzazione, gestione e controllo ex art. 6, c. 1, lett. a), del D.Lgs. 231/2001 esteso nell'ambito di applicazione ai reati previsti dalla L. 190/2012

Informatica Trentina o **Società**: Informatica Trentina S.p.A.

PAT: Provincia Autonoma di Trento

Soggetti apicali: le persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'Ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, nonché persone che esercitano, anche di fatto, la gestione e il controllo aziendale (art. 5, comma 1, lettera a) del D.Lgs. n. 231/2001). Tali soggetti sono stati identificati nei membri del Consiglio di Amministrazione e nel Direttore Generale di Informatica Trentina

Sottoposti: le persone sottoposte alla direzione o alla vigilanza dei Soggetti apicali (art. 5, comma 1, lettera b) del D.Lgs. 231/2001)

Destinatari: Soggetti apicali e Sottoposti

Ente: soggetto fornito di personalità giuridica, società ed associazioni anche prive di personalità giuridica

Organo Dirigente: vedi Soggetti apicali

Organismo di Vigilanza: l'organismo dotato di autonomi poteri di vigilanza e controllo cui è affidata la responsabilità di vigilare sul funzionamento e l'osservanza del Modello 231, avente i requisiti di cui all'art. 6, comma 1, lettera b) del D.Lgs. 231/2001, e di curarne l'aggiornamento

Protocollo: insieme delle procedure aziendali atte a disciplinare uno specifico processo

Responsabile della prevenzione della corruzione e della trasparenza: il soggetto individuato ai sensi dell'art. 1 comma 7 della L. 190/2012

Reati: i reati ai quali si applica la disciplina prevista del D.Lgs. 231/2001 e della L. 190/2012

Sistema Disciplinare: insieme delle misure sanzionatorie applicabili, anche, in caso di violazione del Modello 231

1.3 RIFERIMENTI

Nel presente sono referenziati i seguenti documenti:

- 231-NM "I reati previsti dal D.Lgs. 231/2001";
- 231-RA "Analisi delle attività sensibili ex D.Lgs. 231/2001";
- 231-PTPC "Piano triennale per la prevenzione della corruzione";
- 231-OV "Regolamento dell'Organismo di Vigilanza";
- 231-CE "Codice Etico e di comportamento interno";
- 231-SD-AMM "Sistema disciplinare – Misure nei confronti degli Amministratori";
- 231-PR-WB "Gestione segnalazioni di illeciti e misure a tutela del segnalante".

2 LA NORMATIVA DI RIFERIMENTO

Il D.Lgs. 231/2001, emanato in attuazione della delega di cui all'art. 11 della legge 29 settembre 2000, n. 300, ha inteso conformare la normativa italiana in materia di responsabilità degli enti a quanto stabilito da alcune Convenzioni internazionali ratificate dal nostro Paese.

In particolare, con l'entrata in vigore del D.Lgs. 231/2001 è stata introdotta anche in Italia una forma di responsabilità amministrativa degli enti, quali società, associazioni e consorzi, derivante dalla commissione, o dalla tentata commissione, di alcuni reati, espressamente richiamati dal Decreto stesso, da parte dei Soggetti apicali o dei Sottoposti, nell'interesse o a vantaggio dell'Ente.

La società non risponde, invece, se i predetti soggetti hanno agito nell'interesse esclusivo proprio o di terzi (art. 5, comma 2, D.Lgs. 231/2001).

La responsabilità amministrativa degli enti è autonoma rispetto alla responsabilità penale della persona fisica che ha commesso il reato.

Con la L. 190/2012 e successive integrazioni, lo Stato ha definito una serie di misure per assicurare il controllo, la prevenzione e il contrasto della corruzione e dell'illegalità nella pubblica amministrazione.

In data 24 luglio 2013 è stata sancita l'intesa in sede di Conferenza Unificata Stato – Regioni per l'attuazione dell'art. 1, c. 60 e 61 della L. 190/2012, nella quale sono definiti gli adempimenti e i relativi termini delle Regioni e delle Province autonome di Trento e Bolzano e degli enti locali, nonché degli enti pubblici e dei soggetti di diritto privato sottoposti al loro controllo ai sensi dell'art. 2359 c.c..

Come previsto dal Piano Nazionale Anticorruzione, gli enti di diritto privato in controllo pubblico - categoria di enti nella quale rientra Informatica Trentina - che hanno adottato i modelli di organizzazione e gestione del rischio sulla base del D.Lgs. 231/2001 possono estenderne l'ambito di applicazione a tutti quelli considerati nella L. 190/2012, dal lato attivo e passivo, anche in relazione al tipo di attività svolto dall'ente.

2.1 LE FATTISPECIE DI REATO

La Sezione III del D.Lgs. 231/2001 richiama i reati (documento 231-NM "I reati previsti dal D.Lgs. 231/2001") per i quali è configurabile la responsabilità amministrativa degli enti specificando l'applicabilità delle sanzioni per gli stessi. Alla data di approvazione del presente documento le categorie di reati richiamate sono:

1. Delitti contro la Pubblica Amministrazione;
2. Reati informatici;
3. Delitti di criminalità organizzata;

4. Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento[1];
5. Delitti contro l'industria e il commercio;
6. Reati societari;
7. Reati con finalità di terrorismo o di eversione dell'ordine democratico;
8. Delitti contro la personalità individuale;
9. Reati e illeciti amministrativi di manipolazione del mercato e di abuso di informazioni privilegiate;
10. Reati transnazionali;
11. Reati in materia di salute e sicurezza sul lavoro;[2]
12. Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita;
13. Delitti in materia di violazione del diritto d'autore;
14. Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria;
15. Reati ambientali;
16. Impiego di cittadini di paesi terzi il cui soggiorno è irregolare;
17. Razzismo e xenofobia.

Alle categorie di reati richiamate dal D.Lgs. 231/2001, si aggiungono tutti i reati previsti dalla L.190/2012.

2.2 I MODELLI DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

Il D.Lgs. 231/2001 prevede forme di esonero della responsabilità amministrativa degli enti. In particolare, l'articolo 6 del D.Lgs. 231/2001 stabilisce che, in caso di reato commesso da un Soggetto apicale, l'ente non ne risponde se prova che:

- l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione, gestione e controllo idonei a prevenire reati della specie di quello verificatosi;
- il compito di vigilare sul funzionamento e l'osservanza dei modelli e di curare il loro aggiornamento è stato affidato ad un organismo della società dotato di autonomi poteri di iniziativa e di controllo;
- le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione, gestione e controllo;

[1] Articolo aggiunto dal D.L. 25 settembre 2001 n. 350, art. 6, D.L. convertito con modificazioni dalla legge n. 409 del 23/11/2001; modificato dalla legge n. 99 del 23/07/2009

[2] Articolo aggiunto dalla L. 3 agosto 2007 n. 123, art. 9; modificato dal d. lgs. 3 agosto 2009, n. 106.

- non vi è stata omessa o insufficiente vigilanza da parte dell'organismo preposto.

Pertanto, nel caso di reato commesso da Soggetti apicali, sussiste in capo all'ente una presunzione di responsabilità dovuta al fatto che tali soggetti esprimono e rappresentano la politica e, quindi, la volontà dell'ente stesso. Tale presunzione, tuttavia, può essere superata se l'ente riesce a dimostrare la sussistenza delle succitate quattro condizioni di cui all'art. 6 del D.Lgs. 231/2001.

In tal caso, pur sussistendo la responsabilità personale in capo al Soggetto apicale, l'ente non è responsabile ai sensi del D.Lgs. 231/2001.

Il D.Lgs. 231/2001 attribuisce un valore esimente ai modelli di organizzazione, gestione e controllo nella misura in cui questi ultimi risultino idonei a prevenire i reati di cui al citato Decreto e, al contempo, vengano efficacemente attuati da parte del Consiglio di Amministrazione e della Direzione Generale.

Nello stesso modo, l'art. 7 del D.Lgs. 231/2001 stabilisce la responsabilità amministrativa dell'ente per i reati dei Sottoposti, se la loro commissione è stata resa possibile dall'inosservanza degli obblighi di direzione o di vigilanza. In ogni caso, l'inosservanza di detti obblighi di direzione o di vigilanza è esclusa se l'ente dimostra di aver adottato ed efficacemente attuato, prima della commissione del fatto, un Modello di organizzazione, gestione e controllo idoneo a prevenire reati della specie di quello verificatosi.

Pertanto, nell'ipotesi prevista dal succitato art. 7 del D.Lgs. 231/2001, l'adozione del Modello 231 da parte dell'ente costituisce una presunzione a suo favore, comportando, così, l'inversione dell'onere della prova a carico dell'accusa che dovrà quindi dimostrare la mancata adozione ed efficace attuazione del Modello.

Il Modello 231, per risultare idoneo a prevenire i reati, deve rispondere ai seguenti requisiti:

a) individuare le attività nel cui ambito esiste la possibilità che vengano commessi reati previsti dal Decreto;

b) prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni della società in relazione ai reati da prevenire;

c) individuare modalità di gestione delle risorse finanziarie idonee a impedire la commissione di tali reati;

d) prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza del Modello 231;

e) introdurre un sistema disciplinare interno idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello 231.

2.3 LA SCELTA DI INFORMATICA TRENTINA

L'adozione e l'efficace attuazione del Modello 231 costituiscono, ai sensi dell'art. 6, comma 1, lett. a) del Decreto, atti di competenza e di emanazione dell'organo dirigente.

Sebbene l'adozione di modelli di organizzazione, gestione e controllo sia prevista dal Decreto come facoltativa e non obbligatoria, Informatica Trentina - sensibile all'esigenza di assicurare condizioni di correttezza e di trasparenza nella conduzione degli affari e delle attività aziendali, a tutela della propria posizione e immagine nonché delle aspettative dei propri azionisti e del lavoro dei propri dipendenti – ha ritenuto conforme alle proprie politiche aziendali procedere alla definizione ed all'attuazione del presente Modello 231 e provvedere nel tempo al relativo aggiornamento.

In tale contesto, il Consiglio di Amministrazione di Informatica Trentina con delibera del 6 luglio 2009 ha adottato un proprio Modello organizzativo, di gestione e controllo ai sensi del D.Lgs. 231/2001. Tale Modello definisce principi e regole operative che riprendono ed integrano il più generale modello organizzativo istituito presso la Società.

Con riferimento ai "requisiti" individuati dal legislatore nel Decreto e ulteriormente dettagliati dalle Associazioni di Categoria nelle proprie Linee Guida, le attività che il Consiglio di Amministrazione ha ritenuto di adottare per la predisposizione del Modello 231 sono qui di seguito elencate:

- formalizzazione e diffusione all'interno della propria organizzazione dei principi etici cui la Società ha ispirato da sempre la propria attività;
- analisi ed individuazione dei processi "sensibili" aziendali, ovverosia di quelle attività il cui svolgimento può costituire occasione di commissione dei reati di cui al Decreto e pertanto da sottoporre ad analisi e monitoraggio;
- mappatura specifica ed esaustiva dei rischi derivanti dalle occasioni di coinvolgimento di strutture organizzative aziendali in attività sensibili alle fattispecie di reato;
- individuazione di specifici e concreti protocolli (in essere) con riferimento ai processi sensibili e alle attività aziendali e definizione delle eventuali implementazioni finalizzate a garantire l'adeguamento alle prescrizioni del Decreto;
- identificazione dell'Organismo di Vigilanza secondo criteri di competenza, indipendenza e continuità di azione ed attribuzione al medesimo di specifici compiti di vigilanza sull'efficace e corretto funzionamento del Modello 231 nonché individuazione delle strutture operative in grado di supportarne l'azione;
- definizione dei flussi informativi da/per l'Organismo di Vigilanza;
- definizione delle modalità di formazione e sensibilizzazione del personale;
- definizione e applicazione di disposizioni disciplinari idonee a sanzionare il mancato rispetto delle misure indicate nel Modello 231 e dotate di idonea deterrenza;
- definizione dell'informativa da fornire ai soggetti terzi con cui la Società entri in contatto.

Il compito di vigilare sull'aggiornamento del Modello 231, in relazione a nuove ipotesi di reato o ad esigenze di adeguamento che dovessero rivelarsi necessarie, è affidato dal

Consiglio di Amministrazione all'Organismo di Vigilanza, coerentemente a quanto previsto dall'art. 6, comma 1 lettera b) del Decreto (vedere capitolo 6 "L'Organismo di Vigilanza" a pag. 15).

È cura del Consiglio di Amministrazione e della Direzione Generale procedere all'attuazione del Modello 231.

Per gli adempimenti richiesti dalla L. 190/2012 e dal Piano Nazionale Anticorruzione agli enti di diritto privato in controllo pubblico - categoria di enti nella quale rientra la Società - il Consiglio di Amministrazione di Informatica Trentina integra il proprio Modello organizzativo, di gestione e controllo ai sensi del D.Lgs. 231/2001 con le misure finalizzate a prevenire i fenomeni corruttivi previsti dalla L. 190/2012, dal lato attivo e passivo, in relazione al tipo di attività svolto. Le integrazioni apportate al Modello 231 costituiscono il piano triennale di prevenzione della corruzione.

Il Consiglio di Amministrazione affida al Responsabile della prevenzione della corruzione e della trasparenza (RPCT) i compiti di predisporre ed aggiornare annualmente la proposta di piano triennale per la prevenzione della corruzione e di segnalare le disfunzioni in merito all'attuazione delle misure in materia di prevenzione della corruzione e della trasparenza come previsto dall'art. 1 comma 7 della L. 190/2012. Il RPCT svolge le proprie funzioni in costante coordinamento con quelle dell'Organismo di Vigilanza previsto dall'art. 6 del D.Lgs. 231/2001.

3 LA METODOLOGIA SEGUITA PER L'INDIVIDUAZIONE DELLE ATTIVITÀ SENSIBILI

Sulla base delle attività attualmente svolte e dei reati ricompresi nell'ambito di applicazione del Decreto, in ossequio a quanto previsto dall'art. 6, comma 2, lett. a) del D.Lgs. 231/2001, Informatica Trentina ha provveduto all'individuazione dei processi/attività sensibili, cioè all'identificazione delle attività aziendali concretamente esposte al rischio di commissione di uno dei reati espressamente richiamati dal D.Lgs. 231/2001.

Per l'individuazione delle attività rischiose ex D.Lgs. 231/2001 si è provveduto ad effettuare un'analisi sulla struttura organizzativa allo scopo di far emergere le aree di attività in cui, per contenuto e per interlocutori, vi sia una possibilità di commettere i reati richiamati dal Decreto.

Detta analisi è stata realizzata tramite lo svolgimento di interviste e rilevazioni dirette, effettuate in diversi incontri con il Personale Direttivo e Operativo di Informatica Trentina.

Tali incontri sono stati mirati a:

- individuare le "attività sensibili": vale a dire le attività che risultano interessate da potenziali casistiche di reato;
- analizzare i rischi potenziali: si è proceduto attraverso l'individuazione delle possibili modalità attuative dei reati nelle diverse aree dell'Azienda. L'analisi, propedeutica anche ad una corretta valutazione/progettazione delle misure preventive, è sfociata in una rappresentazione esaustiva di come le fattispecie di reato possano essere attuate rispetto al contesto operativo interno ed esterno a Informatica Trentina;
- valutare il sistema di controlli preventivi: le attività precedentemente descritte si completano con una valutazione del sistema di controlli preventivi e contromisure esistenti, volto a limitare o eliminare i rischi e individuare le aree di potenziale adeguamento, quando ritenuto necessario.

Le descrizioni delle attività sensibili sono state organizzate in un database di riferimento che costituisce il repository dei rischi 231 e che è di supporto nel monitoraggio periodico dei rischi e nel loro aggiornamento.

I risultati dell'analisi sono contenuti nel documento 231-RA "Analisi della attività sensibili ex D.Lgs. 231/2001", documento oggetto di periodica valutazione da parte del C.d.A. di Informatica Trentina e di costante aggiornamento a cura dell'Organismo di Vigilanza.

Per l'integrazione nel Modello 231 delle misure di prevenzione previste dalla L. 190/2012, l'analisi dei rischi è stata estesa all'esposizione ai fenomeni corruttivi; le modalità adottate e i risultati dell'analisi svolta sono contenuti nel documento 231-PTPC "Piano triennale per la prevenzione della corruzione", anch'esso oggetto di periodica valutazione da parte del C.d.A. di Informatica Trentina e di costante aggiornamento a cura del Responsabile della prevenzione della corruzione e della trasparenza.

4 IL MODELLO 231

4.1 I RIFERIMENTI

Il Modello 231 è stato definito avendo come riferimento le Linee Guida in materia emanate dai principali Organismi (Confindustria, ABI, ecc.), Modelli 231 già realizzati nell'ambito di realtà collegate alla PAT, le evidenze dei primi anni di applicazione del Decreto da parte della Magistratura e le esperienze progettuali della Società di consulenza che ha affiancato Informatica Trentina nelle attività operative.

4.2 GLI OBIETTIVI

Con l'introduzione del Modello 231 Informatica Trentina si pone l'obiettivo di strutturare un sistema di elementi organizzativi e relative regole di funzionamento, attraverso l'individuazione delle attività sensibili ex D.Lgs. 231/2001 e ex L. 190/2012 e la definizione di protocolli "idonei a prevenire i reati", volto a:

- rendere consapevoli tutte le persone facenti parte della struttura aziendale, sia di governo sia esecutiva, che eventuali comportamenti illeciti possono comportare sanzioni penali ed amministrative sia per il singolo che per l'azienda;
- garantire la correttezza dei comportamenti dell'azienda e delle persone che la rappresentano, nel completo rispetto della normativa esterna ed interna;
- rafforzare meccanismi di controllo, monitoraggio e sanzionatori atti a contrastare la commissione di reati;
- enfatizzare le scelte in materia di conformità, di etica, di trasparenza, di correttezza da sempre perseguite da Informatica Trentina e peraltro sancite dallo Statuto aziendale, con particolare riferimento alle specifiche finalità della Società nel contesto operativo della Pubblica Amministrazione del Trentino.

4.3 LA STRUTTURA DEL MODELLO 231

Elementi fondamentali del Modello 231 di Informatica Trentina sono:

- il Sistema organizzativo inteso come insieme di responsabilità, processi e prassi operative che disciplinano lo svolgimento delle attività operative, di controllo e di governo dell'azienda. Tali disposizioni, tenuto anche conto delle ridotte dimensioni aziendali, possono essere scritte od orali, di applicazione generale o limitate a categorie di soggetti od individui, permanenti o temporanee. I Destinatari, nello svolgimento delle rispettive attività, si attengono pertanto:
  - alle disposizioni legislative e regolamentari, applicabili alle diverse fattispecie;
  - alle previsioni dello Statuto sociale;

- alle norme generali e alle Linee di condotta emanate ai fini del D.Lgs. 231/2001 e della L. 190/2012;
- alle deliberazioni del Consiglio di Amministrazione;
- alla normativa interna;

- l'Organismo di Vigilanza, inteso come organo dell'ente a cui è affidata la responsabilità di vigilare sul funzionamento e l'osservanza del Modello 231 avente i requisiti di cui all'art. 6 comma 1 lettera b) del D.Lgs. 231/2001 e di curarne l'aggiornamento.

5 IL SISTEMA ORGANIZZATIVO

I controlli coinvolgono, con ruoli e a livelli diversi, il Consiglio di Amministrazione, il Collegio Sindacale, le funzioni di controllo interno, il management e tutto il personale e rappresentano un attributo imprescindibile dell'attività quotidiana della Società.

E' espressa volontà della Società che i protocolli previsti dal Decreto e dalla L. 190/2012, ferma restando la loro finalità peculiare, vadano integrati nel più ampio sistema di controllo interno in essere presso la Società e che pertanto il sistema dei controlli interni esistente sia in grado, con gli eventuali adattamenti che si rendessero necessari, di essere utilizzato anche allo scopo di prevenire i reati contemplati dal Decreto e dalla L. 190/2012.

L'adozione del presente Modello 231 avviene nella convinzione che l'adozione e l'efficace attuazione del Modello non solo consentano alla Società di beneficiare dell'esimente prevista dal D.Lgs. 231/2001, ma migliorino, nei limiti previsti dallo stesso, la sua c*orporate governance*, limitando, anche, il rischio di comportamenti non a norma o che possano avere risvolti in termini di immagine ed economici.

Scopo del Modello 231 è la predisposizione di un sistema strutturato ed organico di procedure ed attività di controllo (preventive e/o ex post) per la prevenzione e consapevole gestione del rischio di commissione dei reati, mediante l'individuazione dei processi sensibili e la loro conseguente proceduralizzazione. Tali attività consentono di:

- determinare, in tutti coloro che operano in nome e per conto della Società nelle "aree di attività a rischio", la consapevolezza di poter incorrere, in caso di violazione delle disposizioni ivi riportate, in un comportamento, sanzionabile sul piano disciplinare e, qualora si configurasse come illecito ai sensi del D.Lgs. 231/2001 e della L. 190/2012, passibile di sanzioni sul piano penale ed amministrativo, non solo nei propri confronti ma anche nei confronti della Società;
- ribadire che qualunque comportamento illecito è fortemente condannato dalla Società in quanto (anche nel caso in cui Informatica Trentina fosse apparentemente in condizione di trarne vantaggio) sono comunque contrarie, oltre che alle disposizioni di legge, anche ai principi etico-sociali cui la Società si attiene nell'espletamento della propria missione aziendale (documento 231-CE "Codice Etico e di comportamento interno");
- consentire ad Informatica Trentina, grazie a un'azione di monitoraggio sui processi/attività sensibili, di intervenire tempestivamente per prevenire o contrastare la commissione dei reati stessi.

5.1 IL SISTEMA DI GESTIONE AZIENDALE

Informatica Trentina ha da tempo definito e documentato il proprio sistema organizzativo ed i relativi meccanismi di funzionamento che vengono costantemente aggiornati per

rispondere alle esigenze strategiche ed organizzative aziendali e per adeguarsi ai requisiti in materia di assetti organizzativi, procedure amministrative richiesti dalla normativa di legge e di settore, nonché alle Direttive emanate dalla PAT.

I principali riferimenti documentali che regolano l'organizzazione interna sono:

- lo Statuto

  lo Statuto costituisce il documento fondamentale su cui è basato il sistema di governo societario: definisce lo scopo dell'azienda, la sede, l'oggetto sociale, il capitale sociale, nonché i compiti e le responsabilità dei Soggetti apicali;

- la documentazione organizzativa aziendale

  descrive la struttura organizzativa e i processi di lavoro aziendali, i compiti e le responsabilità delle unità organizzative; i principali documenti organizzativi aziendali sono rappresentati da:

  - le Comunicazioni interne di variazioni organizzative che disciplinano la struttura delle responsabilità e descrivono l'organigramma aziendale;
  - il Sistema delle deleghe attribuite ai diversi Organi societari;
  - le Delibere del C.d.A.;
  - il Sistema di Gestione per la Qualità composto dal Manuale della qualità, dalle procedure, dalle istruzioni operative e dai documenti correlati;
  - il Sistema di Gestione per la Sicurezza delle Informazioni, composto dalle policy, dalle istruzione operative e dai documenti correlati;
  - il Sistema di Gestione per la Salute e Sicurezza nei luoghi di Lavoro;
  - il Codice Etico e di comportamento interno.

In particolare, con riferimento ai requisiti dell'art. 6 comma 2 del D.Lgs. 231/2001, si è proceduto a verificare la rispondenza del sistema organizzativo ai requisiti di cui alle lettere a), b) e c) di detta norma.

5.2 LE ATTIVITÀ SENSIBILI (EX ART. 6 COMMA 2 LETTERA A)

La mappatura delle attività aziendali "a rischio reato" ex D.Lgs. 231/2001 e L. 190/2012 consente, tra l'altro, di definire i comportamenti che devono essere rispettati nello svolgimento di tali attività, al fine di garantire un sistema di controlli interni idoneo a prevenire la commissione dei reati.

Tali comportamenti devono essere adottati nell'ambito dei processi aziendali, particolarmente in quelli "sensibili". Le regole comportamentali sono parte integrante del Codice Etico (documento 231-CE "Codice Etico e di comportamento interno"); le regole operative sono presenti nella regolamentazione interna di processo nonché rilevabili nelle prassi consolidate.

Per ogni attività a potenziale rischio di commissione di reati sono state approfondite, da parte dei Responsabili delle strutture organizzative coinvolte, le possibili fattispecie di commissione dei reati individuati nello svolgimento delle attività sensibili, l'eventuale coinvolgimento di enti pubblici, la normativa di riferimento, esterna e interna, e le modalità operative in vigore, la presenza ed il livello di efficacia delle attività di controllo e delle altre contromisure organizzative, identificando altresì le eventuali opportunità di miglioramento.

Le risultanze dell'analisi, riassunte nel documento 231-RA "Analisi delle attività sensibili ex D.Lgs. 231/2001" e con le integrazioni contenute nel documento 231-PTPC "Piano triennale per la prevenzione della corruzione", sono validate dalla Direzione Generale e sottoposte periodicamente al Consiglio di Amministrazione e costituiscono punto di riferimento per le attività di integrazione/miglioramento dell'attuale assetto organizzativo e di controllo interno relativamente alle materie di cui al D.Lgs. 231/2001 e alla L. 190/2012.

Con riferimento ai Soggetti apicali, particolarmente esposti ad alcune tipologie di reato per le specifiche responsabilità assegnate, il profilo di rischio del C.d.A. e della Direzione Generale è stato oggetto di una valutazione ai fini della identificazione delle aree di rischio e della sensibilizzazione di ciascun Soggetto Apicale circa la possibile commissione di reati nello svolgimento dei compiti affidati.

5.3 LA FORMAZIONE E L'ATTUAZIONE DEL PROCESSO DECISIONALE (EX ART. 6 COMMA 2 LETTERA B)

Le varie fasi del processo decisionale sono documentate e verificabili, i poteri e le deleghe sono stabiliti dal C.d.A. e resi noti alle strutture organizzative coinvolte.

Nel corso dell'analisi effettuata ai fini del D.Lgs. 231/2001 e della L. 190/2012 è stato espressamente individuato per ogni attività sensibile il riferimento al corpo normativo aziendale, o le prassi in vigore, valutandone il grado di idoneità rispetto alla capacità di prevenzione dei comportamenti illeciti.

In particolare le attività e le decisioni aziendali sono sottoposte a una serie di controlli, da parte del Collegio Sindacale nell'esercizio delle proprie funzioni attribuite ai sensi del codice civile e da parte della Società di Revisione per gli aspetti di natura contabile, oltre a quelli espletati da Informatica Trentina e dalla Provincia Autonoma di Trento.

5.4 LE MODALITÀ DI GESTIONE DELLE RISORSE FINANZIARIE (EX ART. 6 COMMA 2 LETTERA C)

Informatica Trentina ha disciplinato le modalità di gestione delle risorse finanziarie come riportato nella documentazione del sistema delle deleghe attribuite ai diversi Organi societari.

6 L'ORGANISMO DI VIGILANZA

Il Consiglio di Amministrazione di Informatica Trentina ha deliberato di costituire l'Organismo di Vigilanza, previsto dall'art. 6, comma 1, lett. b) del D.Lgs. n. 231/2001, con la responsabilità di vigilare sul funzionamento e l'osservanza del Modello 231, individuare gli eventuali interventi correttivi e proporne l'aggiornamento.

A garanzia delle caratteristiche di indipendenza ed autonomia, l'Organismo di Vigilanza ha natura collegiale ed è costituito da un Consigliere o da un Sindaco avente idonei requisiti di "indipendenza", da una risorsa interna di Informatica Trentina e da un legale esterno.

6.1 NOMINA E DURATA IN CARICA

La nomina dei membri dell'Organismo di Vigilanza è formalizzata mediante apposita delibera del C.d.A., previa valutazione dei requisiti di eleggibilità, professionali e di onorabilità. I membri dell'Organismo di Vigilanza restano in carica per un periodo della durata di tre anni e sono rieleggibili.

L'Organismo di Vigilanza decade alla data della riunione convocata relativa all'ultimo esercizio della sua carica, pur continuando a svolgere ad interim le proprie funzioni fino a nuova nomina dei componenti dell'Organismo stesso.

Qualora uno o più membri dell'Organismo di Vigilanza dovessero decadere così come previsto al successivo par. 6.3, per dimissioni volontarie o per il venir meno della posizione ricoperta nel rapporto con la Società, il C.d.A. provvederà alla loro sostituzione.

6.2 REVOCA MEMBRI DELL'ORGANISMO DI VIGILANZA

La revoca dei poteri propri di uno o più dei membri dell'Organismo di Vigilanza, potrà avvenire soltanto per giusta causa, anche legata ad interventi di ristrutturazione organizzativa della Società, mediante un'apposita delibera del C.d.A..

6.3 CAUSE DI INELEGGIBILITÀ E DECADENZA

Non possono essere nominati membri dell'Organismo di Vigilanza, e se designati decadono:

- coloro i quali abbiano riportato una condanna – anche non definitiva – per uno dei reati previsti dal D.Lgs. 231/2001 ovvero siano stati condannati con sentenza – anche non definitiva; 1) alla reclusione per uno dei delitti previsti nel titolo XI del libro V del codice civile e nel regio decreto del 16 marzo 1942, n. 267; 2) alla reclusione per un tempo non inferiore a un anno per un delitto contro la pubblica amministrazione, contro la fede pubblica, contro il patrimonio, contro l'ordine pubblico, contro l'economia pubblica ovvero per un delitto in materia tributaria; 3)

alla reclusione per un tempo non inferiore a due anni per un qualunque delitto non colposo;

- gli interdetti, gli inabilitati e i falliti;
- i parenti, coniugi o affini con amministratori, sindaci o dipendenti della Società fino al secondo grado incluso.

I membri dell'Organismo di Vigilanza sono tenuti a far conoscere immediatamente al C.d.A. l'eventuale sopravvenienza anche di una sola delle suddette situazioni in quanto comportano la decadenza dall'incarico.

Il venir meno in capo ad un membro della carica di amministratore o sindaco della Società ovvero la risoluzione del rapporto di lavoro subordinato costituisce causa di decadenza dall'incarico.

6.4 COMPITI E FUNZIONI

L'Organismo di Vigilanza è tenuto a:

- promuovere, coordinandosi con le funzioni aziendali competenti, idonee iniziative per la diffusione della conoscenza e della comprensione dei principi del Modello 231, definendo specifici programmi di informazione/formazione e comunicazione interna;
- vigilare sull'effettività del Modello 231, verificando la coerenza tra i comportamenti concreti ed il Modello 231 deliberato, riferendo periodicamente al C.d.A. e al Collegio Sindacale circa lo stato di attuazione del Modello 231;
- definire e comunicare, previa informativa al C.d.A., alle strutture aziendali i flussi informativi che debbono essergli inviati con indicazione dell'unità organizzativa responsabile dell'invio, della periodicità e delle modalità di comunicazione;
- definire e comunicare a tutte le strutture aziendali le modalità con cui effettuare eventuali segnalazioni di comportamenti illeciti o in violazione del Modello 231;
- accertare e segnalare al C.d.A. le violazioni delle previsioni contenute nel Modello 231 ai fini dell'erogazione di eventuali sanzioni a carico dei soggetti che non abbiano rispettato le dette previsioni;
- proporre al C.d.A. l'adozione di eventuali provvedimenti disciplinari nei confronti dei dipendenti a seguito di violazioni del Modello 231;
- valutare l'adeguatezza del Modello 231, ossia la sua reale capacità di prevenire i comportamenti non voluti;
- analizzare il mantenimento nel tempo dei requisiti di solidità e funzionalità del Modello, in particolare con riferimento ai mutamenti ambientali ed alle fattispecie di rischio di nuova insorgenza;

- curare l'aggiornamento del Modello 231 in caso di variazioni della struttura organizzativa, di adeguamenti normativi e di modifiche ai processi aziendali presentando proposte di adeguamento al C.d.A. e verificando l'attuazione e l'effettiva funzionalità delle soluzioni adottate.

Nell'esercizio dei compiti attribuiti l'Organismo di Vigilanza:

- è dotato di autonomi poteri di iniziativa e di controllo, ivi compreso il potere di richiedere e di acquisire informazioni da parte di ogni livello e settore operativo aziendale;
- svolge la sua opera anche attraverso le attività delle diverse funzioni aziendali e/o si avvale, previa richiesta al C.d.A., di soggetti terzi di comprovata professionalità nei casi in cui ciò si renda necessario per l'espletamento delle attività di verifica e controllo, ovvero di aggiornamento del Modello 231;
- è destinatario diretto di eventuali segnalazioni, da parte dei dipendenti, relative alla commissione o al tentativo di commissione dei reati, oltre che di violazione delle regole previste dal Modello 231 stesso.

L'Organismo di Vigilanza riferisce con frequenza almeno annuale al C.d.A. sull'attività svolta e sulla programmazione delle attività di monitoraggio.

In riferimento ai compiti attribuiti all'Organismo di Vigilanza spetta al C.d.A.:

- approvare gli aggiornamenti del modello di organizzazione, gestione e controllo previsto dall'art. 6, comma 1, lett. a) del D.Lgs. 231/2001 (Modello 231);
- approvare il Codice Etico e i successivi aggiornamenti;
- adottare eventuali provvedimenti che dovessero derivare da comportamenti illeciti o violazioni del Modello 231 o del Codice Etico.

6.5 GLI OBBLIGHI DI INFORMAZIONE NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA (EX ART. 6 COMMA 2 LETTERA D)

L'Organismo di Vigilanza ha la responsabilità di vigilare sul funzionamento e l'osservanza del Modello 231 e di provvedere al relativo aggiornamento.

A tal fine l'Organismo di Vigilanza:

- accede a tutti i documenti ed informazioni aziendali rilevanti per lo svolgimento delle funzioni ad esso attribuite;
- può richiedere ai dipendenti e collaboratori di fornire tempestivamente le informazioni, i dati e/o le notizie necessarie per individuare aspetti connessi alle varie attività aziendali rilevanti ai sensi del Modello 231 e per la verifica dell'effettiva attuazione dello stesso;

- riceve periodicamente i flussi informativi definiti, le eventuali comunicazioni da parte dei dipendenti di avvio di procedimento giudiziario a loro carico per reati previsti dal Decreto e dalla L. 190/2012, i rapporti predisposti nell'ambito delle attività di controllo da funzioni interne e/o da soggetti esterni dai quali possano emergere fatti, atti, eventi od omissioni con profili di criticità rispetto alle norme del Decreto e della L. 190/2012.

Al fine di consentire l'inoltro all'Organismo di Vigilanza dei dati, informazioni e documenti richiesti, ovvero per richieste di informazioni in merito al Modello 231, è disponibile lo specifico indirizzo di posta elettronica odv@infotn.it.

Al fine di consentire ai Destinatari del presente Modello 231 di presentare, a tutela dell'integrità della Società, segnalazioni circostanziate di condotte illecite, rilevanti ai sensi del D.Lgs. 231/2001 e fondate su elementi di fatto precisi e concordanti, o di violazione delle regole previste dal Modello 231 stesso, di cui siano venuti a conoscenza in ragione delle funzioni svolte, sono previsti idonei canali di comunicazione nei confronti dell'Organismo di Vigilanza e del Responsabile della prevenzione della corruzione e della trasparenza. Tali canali garantiscono la riservatezza dell'identità del segnalante nelle attività di gestione della segnalazione.

Le segnalazioni possono riguardare anche atti e comportamenti che, anche se non consistenti in specifici reati, contrastano con la necessaria cura dell'interesse pubblico e pregiudicano l'affidamento dei cittadini nell'imparzialità delle amministrazioni e dei soggetti che svolgono attività di pubblico interesse.

La procedura 231-PR-WB "Gestione segnalazioni di illeciti e misure a tutela del segnalante", che ha lo scopo di rimuovere i fattori che possono ostacolare o disincentivare la segnalazione di illeciti e irregolarità, fornisce indicazioni operative in merito a soggetti, oggetto, contenuti, destinatari e modalità di trasmissione delle segnalazioni e descrive le forme di tutela del segnalante contro ritorsioni e discriminazioni.

6.6 ATTRIBUZIONE DI RISORSE FINANZIARIE

L'Organismo di Vigilanza è dotato di un proprio budget di spesa da utilizzare in base alle esigenze emerse nel corso dello svolgimento delle proprie attività; tale utilizzo è lasciato all'autonomia dell'Organismo stesso.

L'Organismo di Vigilanza si può avvalere, previa richiesta al C.d.A., di soggetti terzi di comprovata professionalità nei casi in cui ciò si renda necessario per l'espletamento delle attività di verifica e controllo ovvero di aggiornamento del Modello 231.

6.7 CONSERVAZIONE DELLE INFORMAZIONI

Tutte le comunicazioni verso il C.d.A. e le registrazioni relative alle attività dell'Organismo di Vigilanza ed allo svolgimento delle verifiche devono essere custodite in un apposito

archivio (elettronico o cartaceo) e conservate in luogo sicuro per un periodo di 10 anni. La gestione e custodia dell'archivio è in carico all'Organismo di Vigilanza, fermo restando l'osservanza delle disposizioni in materia di riservatezza dei dati personali e dei diritti da essa garantiti in favore degli interessati.

7 IL SISTEMA DISCIPLINARE (EX ART. 6 COMMA 2 LETTERA E)

Elemento essenziale per il funzionamento del Modello 231 è l'introduzione di un sistema disciplinare idoneo a sanzionare gli eventuali comportamenti contrastanti con le misure previste dal Modello 231. Al riguardo, infatti, l'art. 6 comma 2 lett. e del D.Lgs. 231/2001 prevede che i modelli di organizzazione, gestione e controllo devono "introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello".

L'osservanza delle disposizioni e delle regole comportamentali previste dal Modello 231 costituisce adempimento da parte dei Soggetti sottoposti degli obblighi previsti dall'art. 2104, comma 2, del codice civile, obblighi dei quali il contenuto del Modello 231 rappresenta parte sostanziale ed integrante.

La violazione delle misure indicate nel Modello 231 costituisce un inadempimento contrattuale censurabile sotto il profilo disciplinare ai sensi dell'art. 7 dello Statuto dei lavoratori (legge 20 maggio 1970 n. 300) e determina l'applicazione delle sanzioni previste dal vigente Contratto Collettivo Nazionale dei Lavoratori.

Il mancato rispetto delle misure previste dal Modello 231 viene valutato sotto il profilo disciplinare seguendo modalità differenti a seconda che si tratti di "soggetti sottoposti a direzione o vigilanza" (art. 5, comma 1, lett. b) ovvero di "soggetti apicali" (art. 5, comma 1, lett. a).

L'adeguatezza del sistema disciplinare alle prescrizioni del Decreto e della L. 190/2012 è oggetto di monitoraggio da parte dell'Organismo di Vigilanza.

7.1 LA GESTIONE DEI RAPPORTI IN INFORMATICA TRENTINA

7.1.1 GESTIONE DEI RAPPORTI CON AMMINISTRATORI E SINDACI

Per i Consiglieri di Amministrazione e i Sindaci, Informatica Trentina richiede, al momento dell'assunzione del mandato, l'impegno a rispettare e a dare attuazione al Modello 231 con la previsione che, in caso di violazione del Modello 231, l'Organismo di Vigilanza provvede ad informare il Consiglio di Amministrazione ed il Collegio Sindacale per l'adozione di opportuni provvedimenti.

In particolare, si applicano le disposizioni del documento 231-SD-AMM "Sistema disciplinare – Misure nei confronti degli Amministratori" che regolamenta le modalità di applicazione delle sanzioni nei confronti degli Amministratori nel caso di violazione delle misure di prevenzione della corruzione ex L. 190/2012 o dei protocolli del Modello 231.

7.1.2 GESTIONE DEI RAPPORTI CON I DIPENDENTI

Informatica Trentina provvede ad inserire nelle singole lettere-contratto un'apposita clausola che prevede la sanzionabilità delle condotte contrastanti con le norme di cui al D.Lgs. 231/2001 e alla L. 190/2012 e con il Modello 231 aziendale.

Il sistema sanzionatorio introdotto ai sensi dell'art. 6, comma 2, del Decreto si basa sui principi di immediatezza e tempestività della contestazione della violazione, della concessione di termini per l'esercizio del diritto di difesa prima che la sanzione sia comminata, della proporzionalità della sanzione applicata in relazione alla gravità della violazione commessa ed al grado d'intenzionalità dell'azione o dell'omissione.

In particolare le sanzioni irrogabili nei confronti dei lavoratori sono quelle previste dalla contrattazione collettiva.

7.1.3 GESTIONE DEI RAPPORTI CON I DIRIGENTI

Informatica Trentina provvede ad inserire nelle singole lettere-contratto un'apposita clausola che prevede la sanzionabilità delle condotte contrastanti con le norme di cui al D.Lgs. 231/2001 e alla L. 190/2012 e con il Modello 231 aziendale.

In particolare, in caso di violazione delle procedure interne delle regole e dei principi previsti dal Modello 231 o di adozione nell'espletamento di attività nelle aree a rischio di un comportamento non conforme alle prescrizioni del Modello stesso, si provvederà ad applicare nei confronti dei responsabili le misure più idonee in conformità a quanto previsto dal CCNL per i dirigenti.

7.1.4 GESTIONE DEI RAPPORTI CON I LAVORATORI PARASUBORDINATI E AUTONOMI

Per i collaboratori autonomi e parasubordinati Informatica Trentina adotta, nei singoli contratti, la medesima clausola prevista per i Dirigenti.

Per quanto riguarda, le categorie di lavoratori "atipici" è in ogni caso necessario che venga messo a loro disposizione il Modello 231 e che venga richiesto il puntuale rispetto dei principi in esso contenuti.

7.1.5 GESTIONE DEI RAPPORTI CON PARTI TERZE

La Società, nell'ambito della propria operatività, si avvale della collaborazione di soggetti terzi per la prestazione di servizi e per l'approvvigionamento di beni.

Con riferimento alla gestione dei rapporti con fornitori di beni e/o servizi ed altri soggetti terzi esterni, la Società ha predisposto un apposito modulo da sottoporre per accettazione ai soggetti medesimi in alternativa alla clausola contrattuale, nel quale dichiara di :

- improntare la propria operatività al rispetto assoluto dei più elevati standard di professionalità, integrità, legalità, trasparenza, correttezza e buona fede, ritenendoli condizione imprescindibile ai fini del corretto funzionamento della Società, della tutela della sua affidabilità, reputazione ed immagine, nonché della sempre maggior soddisfazione della propria clientela;
- richiedere ai terzi medesimi comportamenti in linea con quelli adottati dalla Società.

Per quanto riguarda i lavoratori comandati/distaccati, essi saranno soggetti alle regole definite nel Modello 231 di Informatica Trentina che in concreto esercita la direzione/vigilanza, prescindendo dal formale vincolo contrattuale. Ciò posto, il soggetto "comandato", riceve e si attiene al Modello (se previsto) dalla Società presso cui esercita la propria attività (giacché in questo sono indicati i "protocolli" afferenti alle attività nel concreto esercitate).

In ipotesi di lavoratori somministrati da agenzie specializzate (interinali), valgono le seguenti precisazioni:

- nei contratti con le agenzie per il lavoro è opportuno inserire specifiche clausole che impegnino le agenzie medesime ad informare i propri dipendenti, utilizzati dalla Società o che svolgano la loro prestazione presso o in favore di quest'ultima, dei rischi che possono determinare la responsabilità amministrativa della Società stessa, nonché dell'esistenza del Modello 231;
- tali clausole potranno prevedere il recesso o la risoluzione dei contratti stipulati con le agenzie per il lavoro, laddove queste non abbiano adempiuto il predetto onere di informativa dei propri dipendenti;
- sarà, inoltre, espressamente prevista a carico dell'Agenzia per il lavoro, oltre alle clausole di cui sopra, la necessità di applicare le sanzioni disciplinari di cui al sistema sanzionatorio ai dipendenti somministrati nel caso d'inadempimento.

La Società raccomanda alle funzioni responsabili della formalizzazione dei contratti con soggetti terzi di inserire nei rispettivi testi contrattuali specifiche clausole dirette a disciplinare tali conseguenze.

7.2 MISURE APPLICABILI

7.2.1 MISURE NEI CONFRONTI DEGLI AMMINISTRATORI E SINDACI

Vedere quanto previsto nel paragrafo 7.1.1 "Gestione dei rapporti con Amministratori e Sindaci" pag. 20.

7.2.2 MISURE PER I LAVORATORI DIPENDENTI

Con riguardo ai lavoratori dipendenti, il Decreto prevede che il sistema disciplinare deve rispettare i limiti connessi al potere sanzionatorio imposti dall'art. 7 della legge n.

300/1970 (c.d. "Statuto dei lavoratori") e dalla contrattazione collettiva di settore e aziendale, sia per quanto riguarda le sanzioni irrogabili sia per quanto riguarda la forma di esercizio di tale potere.

Il sistema disciplinare correntemente applicato dalla Società, in linea con le previsioni di cui al vigente CCNL, appare munito dei prescritti requisiti di efficacia e deterrenza, in particolare con riferimento al principio secondo il quale, con esplicito riferimento alle previsioni del Decreto e quindi del Modello 231, si sancisce che i lavoratori/lavoratrici che incorrono in violazione degli obblighi ivi previsti sono soggetti a sanzioni disciplinari – oggettivamente e soggettivamente correlate alla gravità dell'infrazione – ai sensi delle norme di legge e contrattuali e del Codice Etico e di comportamento interno adottato dalla Società.

L'istruttoria può essere avviata dal C.d.A. anche su segnalazione motivata dell'Organismo di Vigilanza.

Con riferimento alle sanzioni irrogabili, si precisa che, per quanto ovvio, esse saranno adottate ed applicate nel rispetto delle procedure previste dalle normative collettive nazionali applicabili al rapporto di lavoro, seguendo il previsto iter interno.

7.2.3 MISURE NEI CONFRONTI DEI DIRIGENTI

Vedere quanto previsto nel paragrafo 7.1.3 "Gestione dei rapporti con i Dirigenti" a pag. 21.

7.2.4 MISURE NEI CONFRONTI DELLE PARTI TERZE

Ogni violazione della normativa vigente, del Modello 231 o del Codice Etico e di comportamento da parte di fornitori di beni e/o servizi e altri soggetti esterni con cui la Società entri in contatto nello svolgimento di relazioni d'affari è sanzionata secondo quanto previsto nelle specifiche clausole contrattuali inserite nei relativi contratti.

Resta salva l'eventuale richiesta di risarcimento qualora da tale comportamento derivino danni concreti alla Società, come anche nel caso di applicazione alla stessa da parte del giudice delle misure previste dal Decreto.

7.2.5 MISURE NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA

In caso di violazione dei compiti e delle responsabilità di uno o più dei membri dell'Organismo di Vigilanza, il Consiglio di Amministrazione, accertata l'effettiva inadempienza con il supporto della funzione più appropriata (e nel rispetto della regolamentazione rilevante), provvede a valutare l'opportunità di intraprendere le iniziative più opportune, coerentemente con il profilo aziendale del membro dell'Organismo.

8 LE LINEE DI CONDOTTA 231

Informatica Trentina riconosce come principio imprescindibile il rispetto delle leggi e dei regolamenti vigenti sia di carattere generale sia di settore.

Si precisa che le linee di condotta riportate in questo capitolo:

- non devono ritenersi esaustive, ma sono rappresentative del principio generale di "correttezza e liceità nel lavoro e negli affari";
- fanno riferimento alle aree di attività in cui è stata individuata una possibilità di accadimento dei reati ad oggi richiamati dal Decreto e dalla L. 190/2012 e possono essere considerati principi di riferimento per le estensioni del Decreto a nuove famiglie di reati.

8.1 CONDOTTA NELLA GESTIONE DEI FINANZIAMENTI PUBBLICI

Tutti coloro che operano per conto dell'azienda, senza alcuna distinzione od eccezione, nelle attività di gestione e trattamento di finanziamenti pubblici di qualsivoglia natura ed origine, sono tenuti alla seguente condotta:

- correttezza e "veridicità" nel trattamento della documentazione comprovante i requisiti di ammissibilità per la partecipazione a bandi, gare e consorzi di finanziamenti pubblici;
- correttezza, trasparenza, veridicità e completezza nelle informazioni da fornire all'Amministrazione competente;
- trasparenza e affidabilità delle registrazioni e delle segnalazioni di competenza relative alla gestione ed al trattamento di finanziamenti pubblici;
- integrità e correttezza nell'utilizzo dei finanziamenti pubblici erogati affinché siano destinati allo scopo e secondo le modalità per cui sono stati erogati;
- rispetto della normativa vigente emessa dalle Autorità competenti e della normativa interna.

8.2 CONDOTTA NELLA GESTIONE DEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE

Tutti coloro che, essendo a ciò preposti ed autorizzati, operano per conto di Informatica Trentina a contatto con la Pubblica Amministrazione e con le Istituzioni Pubbliche sono tenuti ad assolvere ai propri compiti con integrità, indipendenza, correttezza e trasparenza.

In particolare le attività devono essere realizzate attenendosi alla seguente condotta:

- divieto di promettere o dare pagamenti o beni, vantaggi o favori illegittimi a Pubblici Ufficiali, o in generale a dipendenti della Pubblica Amministrazione, per promuovere o favorire gli interessi aziendali;
- rispetto dei principi di lealtà, correttezza e trasparenza nelle attività e relazioni in cui siano coinvolti la Pubblica Amministrazione Locale, lo Stato, l'Unione Europea o altri Enti Pubblici in particolare in sede di trattativa, stipula o esecuzione di contratti, aggiudicazione, concessioni o appalti, attività ispettive, di controllo o nell'ambito di procedure giudiziarie e nei casi in cui, svolgendo attività di natura pubblicistica, l'azienda venga ad assumere la veste di Incaricato di Pubblico Servizio;
- osservanza rigorosa delle disposizioni di legge ed interne relative alla "sicurezza dei dati"; questo al fine di prevenire gli eventuali illeciti commessi, a danno della Pubblica Amministrazione Locale, dello Stato, dell'Unione Europea o di altri Enti Pubblici attraverso l'utilizzo di apparati e procedure informatiche messe a disposizione dall'azienda;
- rispetto della legge e trasparenza nei confronti dell'Autorità Giudiziaria nel corso di un eventuale procedimento che veda eventualmente coinvolta la società e durante il quale il dipendente o il dirigente sia chiamato a rilasciare la propria testimonianza.

8.3 CONDOTTA NELL'UTILIZZO DEI SISTEMI INFORMATICI

Tutti coloro che, per posizione e ruolo ricoperto, utilizzano strumenti informatici o telematici per lo svolgimento delle loro attività, sono tenuti alla seguente condotta:

- rispetto della normativa aziendale vigente in materia di trattamento dei dati personali e accesso ai sistemi informatici o telematici;
- correttezza, liceità e integrità nell'utilizzo dei suddetti strumenti protetti da misure di sicurezza;
- correttezza e veridicità delle informazioni contenute nei documenti informatici pubblici o privati scambiati con parti terze.

8.4 CONDOTTA NEGLI ADEMPIMENTI SOCIETARI

Tutti coloro che, per posizione e ruolo ricoperto, assumono, singolarmente o collegialmente decisioni e deliberazioni relative alla gestione della società ed al relativo governo e tutti i dipendenti che a qualunque titolo collaborino in tali attività, sono tenuti alla seguente condotta:

- correttezza, liceità ed integrità, rispetto dei principi normativi e delle regole procedurali interne nella formazione e nel trattamento dei dati, dei documenti contabili e del Bilancio della Società e nella sua rappresentazione all'esterno;

- rispetto dei principi di lealtà, correttezza, collaborazione e trasparenza nelle attività e nelle relazioni con le funzioni ed Autorità di Vigilanza e le Società di revisione;
- applicazione dei principi della riservatezza, della correttezza, della trasparenza, della chiarezza, della veridicità e della completezza nelle attività afferenti la circolazione e la diffusione di notizie che riguardano la Società, sia all'interno che all'esterno;
- rispetto dei principi di correttezza, liceità ed integrità, dei principi normativi e delle regole procedurali interne nella formazione e nel trattamento dei documenti che rappresentano la situazione economica, patrimoniale o finanziaria aziendale.

8.5 CONDOTTA NEI RAPPORTI CON I FORNITORI

Tutti coloro che sono coinvolti nei processi relativi all'acquisto di beni e/o servizi ed in generale nella gestione di rapporti con fornitori sono tenuti alla seguente condotta:

- obiettività nelle selezioni dei fornitori e nella determinazione delle condizioni contrattuali di fornitura;
- rispetto dei principi di lealtà, correttezza e trasparenza nelle attività e relazioni in cui siano coinvolti la Pubblica Amministrazione Locale, lo Stato, l'Unione Europea o altri Enti Pubblici;
- rifiuto di ogni forma di corrispettivo da parte di chiunque per l'esecuzione di un atto relativo al proprio ufficio o contrario ai doveri d'ufficio;
- rispetto della legge, dei regolamenti emessi dalle Autorità competenti e delle procedure interne relative alla gestione delle deleghe dei poteri di spesa;
- rispetto degli obblighi normativi in materia di diritto d'autore e utilizzo delle opere d'ingegno, marchi e brevetti.

8.6 CONDOTTA NEL TRATTAMENTO DELLE INFORMAZIONI

Tutti coloro che, per posizione e ruolo ricoperto, vengono a conoscenza o dispongono, di informazioni privilegiate o comunque riservate, sono tenuti alla seguente condotta:

- rispetto della massima riservatezza con riferimento a informazioni di carattere confidenziale o privilegiato, riguardante la clientela, la Società di cui si sia in possesso in ragione del ruolo ricoperto;
- divieto di utilizzo, nell'interesse proprio o di terzi, delle informazioni di carattere confidenziale o privilegiato di cui al punto precedente;
- divieto di divulgazione delle informazioni di cui al punto precedente a terzi all'interno o all'esterno della Società, salvo il caso in cui tale comunicazione sia necessaria per l'adempimento dei compiti affidati;

- divieto di comunicazione a terzi o sfruttamento a vantaggio proprio o della Società di informazioni finanziarie rilevanti se non dopo che tali informazioni siano state rese pubbliche.

8.7 CONDOTTA IN MATERIA DI SALUTE E SICUREZZA NEI LUOGHI DI LAVORO

Tutti coloro che, per posizione e ruolo ricoperto, sono responsabili di specifici adempimenti o sono coinvolti nei processi relativi alla tutela della salute e sicurezza nei luoghi di lavoro, sono tenuti al rispetto della normativa vigente, in modo particolare all'attuazione degli adempimenti previsti dal D.Lgs. 81/2008, nonché al rispetto dei regolamenti e delle procedure aziendali in materia.

La società si impegna a garantire un ambiente di lavoro conforme alle vigenti norme in materia di salute e sicurezza, promuovendo comportamenti responsabili e preservando, mediante il monitoraggio, la gestione e la prevenzione dei rischi connessi allo svolgimento dell'attività professionale, la salute e la sicurezza di tutti i lavoratori.

8.8 CONDOTTA IN MATERIA DI ANTIRICICLAGGIO

Tutti coloro che sono responsabili di adempimenti in materia di antiriciclaggio, sono tenuti alla seguente condotta:

- rispetto della normativa vigente in materia e delle direttive e regolamenti aziendali;
- rispetto delle procedure in materia di acquisti e spese generali, con particolare riferimento alla verifica dei requisiti dei fornitori e alla provenienza della merce oggetto di acquisto.

9 FORMAZIONE, DIFFUSIONE, RIESAME E AGGIORNAMENTO DEL MODELLO 231

Il Modello 231 è portato a conoscenza di tutti i Destinatari mediante appositi interventi di comunicazione e formazione al fine di garantire la massima diffusione dei principi ispiratori e delle regole di condotta.

Il Modello 231 viene riesaminato periodicamente dall'Organismo di Vigilanza, al fine di verificarne l'effettività, l'adeguatezza, il mantenimento nel tempo dei requisiti di efficacia e funzionalità, curandone il relativo aggiornamento.

L'Organismo nello svolgimento dei suoi compiti si avvale delle competenti strutture aziendali attraverso il coordinamento della Direzione Generale.

L'Organismo riferisce periodicamente al Consiglio di Amministrazione sullo stato di applicazione e sulle eventuali necessità di aggiornamento, proponendo le eventuali integrazioni e/o modifiche del Modello 231.

Il riesame e l'eventuale aggiornamento del Modello 231 è realizzato con cadenza minima annuale, salvo il caso in cui:

- siano introdotti nel D.Lgs. 231/2001 nuovi reati di rilievo per le attività di Informatica Trentina;
- l'azienda svolga nuove attività sensibili o attui significative modifiche organizzative;
- vi siano evidenze di carenze nel Modello 231 che necessitano un tempestivo adeguamento.

Sede legale:
Via G. Gilli, 2
38121 Trento

tel. +39 0461/800111
infotn@pec.infotn.it - infotn@infotn.it - www.infotn.it
odv@infotn.it

Informatica Trentina SpA