MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO EX D. LGS. 8 GIUGNO 2001 N. 231

Approvato dal Consiglio di Amministrazione il 31.03.2016.

IIS CERT srl
Lungo Bisagno Istria, 29/R - 16141 Genova
P.IVA: 01995920996 - Registro Imprese di Genova - REA 451423

INDICE

SEZIONE PRIMA

1. IL DECRETO LEGISLATIVO 8 GIUGNO 2001 N. 231

1.1. LA RESPONSABILITÀ AMMINISTRATIVA DEGLI ENTI

Il D. Lgs. 8 giugno 2001, n. 231, recante la "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica" (di seguito anche il "**D. Lgs. 231/2001**" o **Decreto**), entrato in vigore il 4 luglio 2001 in attuazione dell'art. 11 della Legge Delega 29 settembre 2000 n. 300, ha introdotto nell'ordinamento giuridico italiano, conformemente a quanto previsto in ambito comunitario, la responsabilità amministrativa degli enti, ove per "enti" si intendono le società commerciali, di capitali e di persone, e le associazioni, anche prive di personalità giuridica.

Tale nuova forma di responsabilità, sebbene sia definita "amministrativa" dal legislatore, presenta i caratteri propri della responsabilità penale, essendo rimesso al giudice penale competente l'accertamento dei reati dai quali essa è fatta derivare, ed essendo estese all'ente le medesime garanzie del processo penale.

La responsabilità amministrativa dell'ente deriva dal compimento di reati, espressamente indicati nel D. Lgs. 231/2001, commessi, nell'interesse o a vantaggio dell'ente, da persone fisiche che rivestano funzioni di rappresentanza, amministrazione o direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, o che ne esercitino, anche di fatto, la gestione e il controllo (i cosiddetti "**soggetti apicali**"), ovvero che siano sottoposte alla direzione o vigilanza di uno dei soggetti sopra indicati (i cosiddetti "**sottoposti**").

Oltre all'esistenza dei requisiti sopra descritti, il D. Lgs. 231/2001 richiede anche l'accertamento della colpevolezza dell'ente, al fine di poterne affermare la responsabilità. Tale requisito è riconducibile ad una "colpa di organizzazione", da intendersi quale mancata adozione, da parte dell'ente, di misure preventive adeguate a prevenire la commissione dei reati di cui al successivo paragrafo, da parte dei soggetti espressamente individuati dal Decreto.

Laddove l'ente sia in grado di dimostrare di aver adottato ed efficacemente attuato un'organizzazione idonea ad evitare la commissione di tali reati, attraverso l'adozione del modello di organizzazione, gestione e controllo previsto dal D. Lgs. 231/2001, questi non risponderà a titolo di responsabilità amministrativa.

1.2. I REATI PREVISTI DAL DECRETO

Per il contenuto di questa sezione si rimanda all'identica sezione del Modello di IIS Ente Morale n. 1.2. rinvenibile sul sito www.iis.it.

1.3. LE SANZIONI COMMINATE DAL DECRETO

Per il contenuto di questa sezione si rimanda all'identica sezione del Modello di IIS Ente Morale n. 1.3. rinvenibile sul sito www.iis.it.

1.4. CONDIZIONE ESIMENTE DELLA RESPONSABILITÀ AMMINISTRATIVA

Introdotta la disciplina concernente la responsabilità amministrativa dell'ente, l'art. 6 del D. Lgs. 231/2001 stabilisce che lo stesso non risponde a titolo di responsabilità amministrativa, qualora dimostri 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 curarne il relativo aggiornamento, è stato affidato ad un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo (c.d. Organismo di Vigilanza);
- le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione gestione e controllo;
- non vi è stata omessa o insufficiente vigilanza da parte dell'Organismo di Vigilanza.

L'adozione del modello di organizzazione, gestione e controllo, dunque, è condizione necessaria perché l'ente possa sottrarsi all'imputazione di responsabilità amministrativa. La mera adozione di tale documento, con delibera dell'organo amministrativo dell'ente, da individuarsi nel Consiglio di Amministrazione, non è, tuttavia, sufficiente ad escludere *tout court* detta responsabilità, essendo necessario che il modello sia efficacemente attuato da parte dell'ente e dallo stesso effettivamente applicato.

Con riferimento all'efficacia del modello di organizzazione, gestione e controllo per la prevenzione della commissione dei reati previsti dal D. Lgs. 231/2001, si richiede che esso:

- individui, mediante specifica ed esaustiva attività di mappatura dei rischi, le attività nel cui ambito possono essere commessi i reati;

- preveda specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;
- individui modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati;
- preveda obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli;
- introduca un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello di organizzazione, gestione e controllo.

Con riferimento all'effettiva applicazione del modello di organizzazione, gestione e controllo, il D. Lgs. 231/2001 richiede:

- un sistema di verifiche sia periodiche sia a sorpresa, e, nel caso in cui siano scoperte significative violazioni delle prescrizioni imposte dal modello o intervengano mutamenti nell'organizzazione o nell'attività dell'ente ovvero modifiche legislative, la modifica del modello di organizzazione, gestione e controllo;
- l'irrogazione di sanzioni in caso di violazione delle prescrizioni imposte dal modello di organizzazione, gestione e controllo, e quindi un sistema disciplinare idoneo a sanzionare il mancato rispetto dello stesso.

1.5. LE "LINEE GUIDA" DI CONFINDUSTRIA

Per il contenuto di questa sezione si rimanda all'identica sezione del Modello di IIS Ente Morale n. 1.5. rinvenibile sul sito www.iis.it.

SEZIONE SECONDA

2. IL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO DI IIS CERT

2.1. FINALITÀ DEL MODELLO

IIS CERT è società del Gruppo IIS ed opera dalla sede centrale di Genova, nonchè dagli uffici regionali e/o unità distaccate di Legnano (MI), Mogliano Veneto (TV), Priolo Gargallo (SR) e le unità distaccate di Modena (MO), Taranto (TA) e Roma (RM).

I servizi di IIS CERT, come esplicitati in Statuto, riguardano la valutazione di conformità, secondo i principali codici e normative nazionali ed internazionali, di: i) personale; ii) sistemi di gestione qualità, ambiente e sicurezza; iii) processi e procedure di fabbricazione e controllo; iv) prodotti e materiali.

IIS CERT è Ente Notificato a Bruxelles con numero NB 0475.

Come Organismo di Certificazione IIS CERT opera con accreditamenti dell'Ente Nazionale di Accreditamento ACCREDIA, con gli accreditamenti ministeriali, con autorizzazioni dell'European Welding Federation (EWF), dell'International Institute of Welding (IIW), nonché dell'Agenzia Nazionale per la Sicurezza delle Ferrovie (ANSF), come da documento CER QAS 059,

Inoltre IIS CERT è il socio di riferimento del CEC (Consorzio Europeo Certificazione), attraverso il quale svolge attività di valutazione di conformità dei prodotti ai sensi delle Direttive PED e TPED, nonché verifiche periodiche su attrezzature in servizio ai sensi della legislazione vigente in materia di utilizzo in sicurezza delle stesse.

IIS CERT ha approvato il presente modello di organizzazione, di gestione e controllo con delibera del Consiglio di Amministrazione del 31.03.2016.

IIS CERT è infatti sensibile all'esigenza di assicurare condizioni di correttezza e trasparenza nella conduzione degli affari e delle attività aziendali, a tutela della propria posizione e immagine, e del lavoro dei propri dipendenti ed è, altresì, consapevole dell'importanza di dotarsi di un modello di organizzazione, gestione e controllo (di seguito il "**Modello**"), idoneo a prevenire la commissione di comportamenti illeciti da parte dei propri amministratori, dipendenti e collaboratori sottoposti a direzione o vigilanza da parte della Società.

2.2. DESTINATARI

Le disposizioni del presente Modello sono, dunque, vincolanti per gli amministratori e per tutti coloro che rivestono funzioni di rappresentanza, amministrazione e direzione anche di fatto di IIS CERT, per i dipendenti (per tali intendendosi tutti coloro che sono legati a IIS CERT da un rapporto di lavoro subordinato, incluso il personale dirigente), per i collaboratori esterni sottoposti alla direzione o vigilanza del management aziendale della IIS CERT (di seguito i "**Destinatari**").

2.3. ELEMENTI FONDAMENTALI DEL MODELLO

Con riferimento alle esigenze individuate nel D. Lgs. 231/2001, gli elementi fondamentali sviluppati da IIS CERT nella definizione del Modello, possono essere così riassunti:

- mappatura delle attività sensibili, con esempi di possibili modalità di realizzazione dei reati e dei processi strumentali potenzialmente associabili alla commissione dei reati richiamati dal Decreto, da sottoporre, pertanto, ad analisi e monitoraggio periodico;
- identificazione dei principi etici e delle regole comportamentali volte alla prevenzione di condotte che possano integrare le fattispecie di reato previste dal D. Lgs. 231/2001, sancite nel Codice Etico adottato dal Gruppo IIS, e, più in dettaglio, nel presente Modello;
- previsione di specifici protocolli relativi ai processi strumentali ritenuti a maggior rischio potenziale di commissione di reato, diretti a regolamentare espressamente la formazione e l'attuazione delle decisioni di IIS CERT, al fine di fornire indicazioni specifiche sul sistema di controlli preventivi in relazione alle singole fattispecie di illecito da prevenire;
- nomina di un Organismo di Vigilanza collegiale (di seguito anche "**Organismo**" o "**OdV**"), e attribuzione di specifici compiti di vigilanza sull'efficace attuazione ed effettiva applicazione del Modello;
- approvazione di un sistema sanzionatorio idoneo a garantire l'efficace attuazione del Modello, contenente le disposizioni disciplinari applicabili in caso di mancato rispetto delle misure indicate nel Modello medesimo;
- svolgimento di un'attività di informazione e formazione ai Destinatari del presente Modello;
- modalità per l'adozione e l'effettiva applicazione del Modello nonché per le necessarie modifiche o integrazioni dello stesso (aggiornamento del Modello).

2.4. CODICE ETICO E MODELLO

IIS CERT, al fine di conformare le proprie attività a principi etici diretti ad improntare le attività aziendali al rispetto delle leggi e regolamenti vigenti in Italia e in tutti i Paesi in cui opera, ha da tempo adottato il Codice Etico del Gruppo IIS, che sancisce i principi di "deontologia aziendale" che IIS CERT riconosce come propri.

IIS CERT esige l'osservanza dei principi etici contenuti nel Codice Etico da parte di tutti coloro che agiscono in nome e per conto dello stesso e, più in generale, di tutti coloro che, a qualsiasi titolo, entrino in relazione di affari con esso.

Il Codice Etico ha, pertanto, una portata di carattere generale e rappresenta un insieme di regole, adottate spontaneamente da IIS CERT, che la stessa riconosce, accetta e condivide, dirette a diffondere una solida integrità etica ed una forte sensibilità al rispetto delle normative vigenti.

Il Modello risponde, invece, a specifiche prescrizioni contenute nel D. Lgs. 231/2001, finalizzate espressamente a prevenire la commissione delle tipologie di reati previste dal Decreto medesimo (per fatti che, apparentemente commessi nell'interesse o a vantaggio di IIS CERT, possono far sorgere a carico della stesso una responsabilità amministrativa da reato).

In considerazione del fatto che il Codice Etico richiama principi di comportamento idonei anche a prevenire i reati di cui al D. Lgs. 231/2001, tale documento acquisisce rilevanza ai fini del Modello e costituisce, pertanto, un elemento complementare allo stesso e un valido strumento di prevenzione delle fattispecie penali ricomprese nel Decreto.

2.5. PRESUPPOSTI DEL MODELLO

Il D. Lgs. 231/2001 prevede espressamente, al relativo art. 6, comma 2, lett. a), che il Modello di Organizzazione, Gestione e Controllo di IIS CERT individui le attività aziendali nel cui ambito possano essere potenzialmente commessi i reati inclusi nel Decreto.

Di conseguenza, IIS CERT ha proceduto ad una approfondita analisi delle proprie attività aziendali.

Nell'ambito di tali attività, IIS CERT ha, in primo luogo, analizzato la propria struttura organizzativa, rappresentata nell'organigramma aziendale, che individua le Funzioni aziendali, evidenziandone ruoli e linee gerarchiche.

Successivamente, IIS CERT ha proceduto alla specifica mappatura dei rischi potenzialmente connessi all'esercizio delle proprie attività aziendali sulla base delle informazioni raccolte dai

referenti aziendali (Responsabili di Funzione) che, in ragione del ruolo ricoperto, risultano provvisti della più ampia e profonda conoscenza dell'operatività del settore aziendale di relativa competenza.

I risultati dell'attività sopra descritta sono stati raccolti in una scheda descrittiva (c.d. **Matrice delle Attività a Rischio-Reato**), che illustra in dettaglio i profili di rischio di commissione dei reati richiamati dal D. Lgs. 231/2001, nell'ambito delle attività proprie del Gruppo IIS. Detta Matrice delle Attività a Rischio-Reato è custodita presso la sede di IIS Ente Morale dal Presidente di IIS CERT (Segretario Generale di IIS Ente Morale), che ne cura l'archiviazione, rendendola disponibile per l'eventuale consultazione agli amministratori, ai sindaci, all'Organismo di Vigilanza e a chiunque sia legittimato a prenderne visione.

In particolare, nella Matrice delle Attività a Rischio-Reato vengono rappresentate le aree aziendali a potenziale rischio di commissione dei reati previsti dal D. Lgs. 231/2001 (c.d. "**attività sensibili**"), i reati associabili, gli esempi di possibili modalità a finalità di realizzazione degli stessi, nonché i processi nel cui svolgimento, sempre in linea di principio, potrebbero crearsi le condizioni, gli strumenti e/o i mezzi per la commissione dei reati stessi (c.d. "**processi strumentali**").

Quanto sopra detto, si è ritenuto di redigere il Modello, per IIS CERT e per ciascuna delle altre entità del Gruppo, secondo il seguente schema logico-funzionale:

Codice Etico:	Comune all'intero Gruppo IIS;
Modello in "Parte Generale":	Per IIS Ente Morale e per ciascuna delle Società;
Matrice di Rischio:	Comune all'intero Gruppo IIS; in essa, sia le singole attività "a rischio/reato presupposto" (dirette e strumentali) sia l'indicazione degli strumenti a presidio della commissione di reati sono descritte e riferite alla/e singola/e entità (IIS Ente Morale o Società del Gruppo IIS) presso cui sono effettivamente svolte, anche se tali entità sono diverse fra loro. Ritenendo gli estensori del Modello che la separazione di funzioni e attività fra le diverse entità del Gruppo IIS, se correttamente attuata, possa utilmente fungere da presidio contro la commissione di reati/presupposto. Ad. es: il rischio/reato ex art. 2635 comma 3 c.c. (corruzione fra privati) realizzabile mediante l'emissione di falsi certificati

sarà indicato come "potenziale" in IIS CERT. Il relativo presidio è invece indicato sia in capo a IIS Ente Morale (struttura del sistema informatico di Gruppo che impedisce ai funzionari tecnici di emettere la documentazione di certificazione) sia in capo a una diversa funzione della stessa IIS CERT (necessità di riesame da parte dell'organo deliberante).

Protocolli di prevenzione: per ciascuna delle entità costituenti il Gruppo IIS sono previsti protocolli (regole organizzative/operative di comportamento) rispetto ai rischi/reato riferibili alla/e singola/ entità.

2.5.1. ATTIVITÀ A RISCHIO-REATO

Nello specifico, è stato riscontrato il rischio di potenziale commissione dei reati previsti dal D. Lgs. 231/2001 nelle seguenti aree di attività aziendale, che vengono di seguito riportate come indicate nella Matrice delle Attività a Rischio-Reato:

A. Rapporti di profilo istituzionale con soggetti appartenenti alla Pubblica Amministrazione;
B. Gestione dei rapporti con gli Enti Pubblici competenti in occasione dell'espletamento degli adempimenti connessi all'attività sociale, anche in occasione di verifiche ed ispezioni;
C. Gestione dell'ideazione, produzione e commercializzazione dei servizi;
D. Espletamento degli adempimenti previsti nell'ambito della gestione delle attività estere;
E. Acquisizione e gestione di contratti con Enti Pubblici nello svolgimento dell'attività caratteristica, mediante partecipazione a procedure ad evidenza pubblica, procedure negoziate (già trattative private) ed affidamenti diretti;
F. Gestione ed esecuzione dei contratti con i clienti/Enti Pubblici, anche in sede di verifiche ed ispezioni;
G. Gestione del sistema Sicurezza ai sensi del D. Lgs. 81/08 (Testo Unico Sicurezza);
H. Gestione degli adempimenti richiesti dalla normativa vigente non connessi all'attività caratteristica, anche in occasione di verifiche, ispezioni e accertamenti da parte degli Enti Pubblici competenti o delle Autorità di Vigilanza;
I. Gestione degli adempimenti necessari alla richiesta di finanziamenti e/o agevolazioni e predisposizione della relativa documentazione;

J. Gestione degli adempimenti in materia di assunzioni, cessazione del rapporto di lavoro, retribuzioni, ritenute fiscali e contributi previdenziali e assistenziali, relativi a dipendenti e collaboratori;

K. Gestione dei contenziosi giudiziali e stragiudiziali (es. Civili, tributari, giuslavoristici, amministrativi, penali), in tutti i gradi di giudizio, nomina dei professionisti esterni e coordinamento delle relative attività;

L. Gestione, utilizzo e manutenzione del sistema informativo aziendale;

M. Coordinamento e gestione della contabilità generale e formazione del bilancio;

N. Adempimenti societari.

In considerazione delle aree di attività di rischio aziendale sopra riportate sono risultati potenzialmente realizzabili nel contesto aziendale di IIS CERT i reati di cui agli artt. 24, 24 bis, 25, 25 bis, 25 bis 1, 25 ter, 25 septies, 25 octies 25 novies e 25 decies.

Il rischio di commissione dei reati di cui agli artt. 24 *ter*, 25 *bis*, 25 *quater*, 25 *quater 1*, 25 *quinquies* e 25 *sexies*, nonché dei reati transnazionali previsti dall'art. 10 della Legge 146/2006, per quanto non si possa escludere *tout court*, è stato ritenuto estremamente remoto in considerazione delle attività svolte da IIS CERT ed in ogni caso ragionevolmente coperto dal rispetto dei principi etici e delle regole comportamentali enunciate nel Codice Etico adottato da IIS CERT, che vincola tutti i suoi destinatari alla più rigorosa osservanza delle leggi e delle normative ad essa applicabili.

2.5.2. PROCESSI STRUMENTALI

Sono stati anche individuati i processi c.d. strumentali nel cui ambito, in linea di principio, potrebbero crearsi le condizioni e/o potrebbero essere forniti gli strumenti per la commissione delle fattispecie di reato:

1. Gestione degli acquisti di beni, servizi e consulenze (ivi compresi gli incarichi professionali);
2. Gestione di donazioni, sponsorizzazioni e omaggi;
3. Selezione, assunzione e gestione del personale dipendente (ivi compresi i rimborsi spese e le spese di rappresentanza;
4. Gestione della produzione e della qualità del prodotto;
5. Gestione delle visite ispettive e dei rapporti con la Pubblica Amministrazione;

6. Gestione della contabilità (e dei flussi finanziari), della formazione del bilancio e rapporti con gli organi sociali;
7. Gestione delle vendite e dei contratti verso clienti pubblici e degli agenti;
8. Gestione degli adempimenti in materia di salute e sicurezza nei luoghi di lavoro;
9. Gestione della sicurezza e manutenzione dei sistemi informativi;
10. Gestione dei finanziamenti pubblici.

2.6. SISTEMA DI CONTROLLO INTERNO

Nella predisposizione del Modello, IIS CERT ha tenuto conto del Sistema di Controllo Interno esistente in azienda, al fine di verificare se esso fosse idoneo a prevenire gli specifici reati previsti dal Decreto nelle aree di attività a rischio identificate.

Il sistema di controllo coinvolge ogni settore dell'attività svolta da IIS CERT attraverso la distinzione dei compiti operativi da quelli di controllo, riducendo ragionevolmente ogni possibile conflitto di interesse.

In particolare, il sistema di controllo interno di IIS CERT si basa, oltre che sulle regole comportamentali previste nel presente Modello, anche sui seguenti elementi:

- il Codice Etico;
- il sistema di protocolli di prevenzione/procedure aziendali;
- la struttura gerarchico-funzionale (organigramma aziendale);
- il sistema di deleghe e procure;
- documenti di governance;
- manuali di gestione.
- sistemi informativi integrati e orientati alla segregazione delle funzioni e alla protezione delle informazioni in essi contenute, con riferimento sia ai sistemi gestionali e contabili che ai sistemi utilizzati a supporto delle attività operative connesse al business.

I principi che regolano le attività nelle aree a rischio e nei processi precedentemente illustrati sono i seguenti:

- esistenza di regole comportamentali di carattere generale a presidio delle attività svolte;

- esistenza e adeguatezza di procedure per la regolamentazione dello svolgimento delle attività nel rispetto dei principi di: tracciabilità degli atti, oggettivazione del processo decisionale e previsione di adeguati punti di controllo;
- rispetto e attuazione concreta del generale principio di separazione dei compiti, secondo cui nessuno deve poter gestire un intero processo in autonomia;
- esistenza di livelli autorizzativi a garanzia di un adeguato controllo del processo decisionale, supportato da un sistema di deleghe e procure riguardante sia i poteri autorizzativi interni, dai quali dipendono i processi decisionali dell'azienda in merito alle operazioni da porre in essere, sia i poteri di rappresentanza per la firma di atti o documenti destinati all'esterno e idonei a vincolare IIS CERT nei confronti dei terzi (cosiddette "procure" speciali o generali);
- sistema di comunicazione interna e formazione del personale;
- esistenza di specifiche attività di controllo e di monitoraggio.

La responsabilità, in ordine al corretto funzionamento del sistema dei controlli interni, è rimessa a ciascuna Funzione per tutti i processi di cui essa sia responsabile.

La tipologia di struttura dei controlli aziendali esistente in IIS CERT prevede:

- controlli interni di governance, controlli interni QSA, controlli interni da parte di soggetti esterni (Accredia, Ministeri).
- controlli di linea, svolti dalle singole Funzioni sui processi di cui hanno la responsabilità gestionale, finalizzati ad assicurare il corretto svolgimento delle operazioni;
- attività di monitoraggio, svolta dai responsabili di ciascun processo e volte a verificare il corretto svolgimento delle attività sottostanti.

Tutto il personale, nell'ambito delle funzioni svolte, è responsabile della definizione e del corretto funzionamento del sistema di controllo, costituito dall'insieme delle attività di verifica che le singole funzioni svolgono sui loro processi.

2.7. REGOLE COMPORTAMENTALI DI CARATTERE GENERALE

Di seguito si rappresentano le regole comportamentali di carattere generale che devono essere osservate al fine di prevenire il rischio di commissione dei reati rilevanti ai sensi del Decreto

identificato. La violazione di dette regole comporterà l'applicazione delle misure sanzionatorie previste nella sezione Quarta.

2.7.1. COMPORTAMENTI DA TENERE NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE E CON LE AUTORITÀ DI VIGILANZA

Le seguenti regole di comportamento di carattere generale si applicano ai Destinatari del presente Modello che, a qualunque titolo, intrattengano rapporti con la Pubblica Amministrazione o con le Autorità di Vigilanza per conto o nell'interesse di IIS CERT.

In via generale, ai Destinatari è fatto divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino o possano integrare, direttamente o indirettamente, le fattispecie di reato previste dagli artt. 24 e 25 del D. Lgs. 231/2001.

In particolare, coerentemente con i principi deontologici aziendali di cui al presente Modello e al Codice Etico adottato da IIS CERT, è fatto divieto di:

- promettere o effettuare erogazioni in denaro a favore di rappresentanti della Pubblica Amministrazione o delle Autorità di Vigilanza, per finalità diverse da quelle istituzionali e di servizio;
- promettere o concedere vantaggi di qualsiasi natura (es.: promesse di assunzione) in favore di rappresentanti della Pubblica Amministrazione e Autorità di Vigilanza, italiane o straniere, al fine di influenzarne l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio a IIS CERT;
- effettuare prestazioni o pagamenti in favore di collaboratori, fornitori, consulenti, o altri soggetti terzi che operino per conto di IIS CERT, che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi ovvero in relazione al tipo di incarico da svolgere ed alle prassi vigenti in ambito locale;
- favorire, nei processi di acquisto, collaboratori, fornitori, consulenti o altri soggetti terzi in quanto indicati da rappresentanti della Pubblica Amministrazione o delle Autorità di Vigilanza;
- accordare omaggi e regali al di fuori di quanto previsto dalla prassi aziendale (vale a dire ogni forma di regalo offerto eccedente le normali pratiche commerciali o di cortesia, o comunque rivolto ad acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale). In particolare, è vietata qualsiasi forma di regalo o altra utilità a funzionari pubblici o a loro familiari, che possa influenzarne l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per IIS CERT. Gli omaggi consentiti si caratterizzano

sempre per l'esiguità del loro valore. Eventuali omaggi devono essere autorizzati e in ogni caso adeguatamente documentati per consentire le verifiche da parte dell'Organismo di Vigilanza;

- tenere una condotta ingannevole che possa indurre la Pubblica Amministrazione o l'Autorità di Vigilanza in errore di valutazione tecnico-economica sulla documentazione presentata;
- esibire documenti o dati falsi o alterati ovvero rendere informazioni non corrispondenti al vero;
- omettere informazioni dovute al fine di orientare a proprio favore le decisioni della Pubblica Amministrazione o delle Autorità di Vigilanza;
- presentare dichiarazioni non veritiere a organismi Pubblici nazionali o comunitari al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati;
- destinare somme ricevute da organismi Pubblici nazionali o comunitari a titolo di erogazioni, contributi o finanziamenti per scopi diversi da quelli cui erano destinati.

IIS CERT condanna ogni condotta che possa, in qualsivoglia modo, integrare, direttamente o indirettamente, il reato di "Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria" e/o agevolarne o favorirne la relativa commissione. In particolare è fatto divieto di:

- promettere o offrire erogazioni in denaro o di altra utilità a favore di soggetti coinvolti in procedimenti giudiziari al fine di indurlo ad occultare/omettere fatti che possano arrecare pene/sanzioni a IIS CERT;
- indurre un soggetto a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria nel corso di un procedimento penale, attraverso minaccia o violenza (coazione fisica o morale) al fine di occultare/omettere fatti che possano arrecare pene/sanzioni a IIS CERT.

In particolare, è fatto obbligo ai Destinatari di attenersi alle seguenti prescrizioni:

- i rapporti con la Pubblica Amministrazione devono essere gestiti procedendo all'identificazione dei responsabili di riferimento per le attività svolte su tali aree a rischio;
- gli incarichi conferiti ai collaboratori esterni (es. fornitori, consulenti) devono essere redatti per iscritto, con indicazione dell'oggetto dell'incarico, del compenso pattuito ed essere sottoscritti conformemente alle deleghe ricevute;

- sono vietate forme di pagamento in contanti o in natura, fatta eccezione per casi straordinari adeguatamente motivati.

Coloro che svolgono una funzione di controllo e supervisione su adempimenti connessi all'espletamento delle suddette attività (pagamento di fatture, destinazione di finanziamenti ottenuti dallo Stato o da organismi comunitari, ecc.) devono porre particolare attenzione sull'attuazione degli adempimenti stessi e riferire immediatamente all'Organismo di Vigilanza presunte situazioni di irregolarità o di non conformità eventualmente riscontrate.

Da ultimo, è fatto obbligo ai Destinatari dei presenti principi etico - comportamentali di attenersi alle seguenti prescrizioni: in caso di presunta tentata concussione da parte di un pubblico funzionario (da intendersi quale abuso della qualità o potere da parte di un funzionario pubblico al fine di costringere o indurre taluno a dare o promettere, allo stesso o a un terzo, denaro o altre utilità non dovute per lo svolgimento dei relativi doveri d'ufficio), il soggetto interessato deve: (i) non dare seguito alla richiesta; (ii) fornire tempestivamente informativa all'Organismo di Vigilanza.

2.7.2. COMPORTAMENTI DA TENERE NELL'AMBITO DELLE ATTIVITÀ "SENSIBILI" RISPETTO AI REATI SOCIETARI

I seguenti principi di comportamento di carattere generale si applicano ai Destinatari del presente Modello che, a qualunque titolo, siano coinvolti nelle attività "sensibili" rispetto ai reati societari di cui all'art. 25 *ter* del D. Lgs. 231/2001.

In via generale, a tali soggetti è richiesto di:

- tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire al socio e al pubblico un'informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria di IIS CERT;
- garantire la massima collaborazione all'Organismo di Vigilanza e alla Dirigenza Aziendale, assicurando completezza e chiarezza delle informazioni fornite, nonché l'accuratezza dei dati e delle elaborazioni, con segnalazione di eventuali conflitti d'interessi;
- osservare rigorosamente tutte le norme poste dalla legge a tutela dell'integrità ed effettività del capitale sociale, al fine di non ledere le garanzie dei creditori e dei terzi in genere;
- assicurare il regolare funzionamento di IIS CERT e degli organi sociali, garantendo ed agevolando ogni forma di controllo interno sulla gestione sociale previsto dalla legge;

- effettuare con tempestività, correttezza e buona fede tutte le comunicazioni previste dalla legge nei confronti delle Autorità Amministrative Indipendenti, non frapponendo alcun ostacolo all'esercizio delle funzioni dalle stesse esercitate.

È inoltre previsto l'espresso obbligo a carico dei soggetti sopra indicati, qualora se ne configuri l'applicabilità, di evitare di:

- porre in essere operazioni simulate o diffondere notizie false su IIS CERT nonché sulla sua attività;
- rappresentare o trasmettere per l'elaborazione e la rappresentazione in bilanci, relazioni o altre comunicazioni sociali, dati falsi, lacunosi o, comunque, non rispondenti alla realtà, sulla situazione economica, patrimoniale e finanziaria di IIS CERT;
- omettere dati ed informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria di IIS CERT;
- restituire conferimenti al socio o liberare lo stesso dall'obbligo di eseguirli, al di fuori dei casi di legittima riduzione del capitale sociale;
- ripartire utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva;
- acquistare o sottoscrivere quote di IIS CERT fuori dai casi previsti dalla legge, con lesione all'integrità del capitale sociale;
- effettuare riduzioni del capitale sociale, fusioni o scissioni, in violazione delle disposizioni di legge a tutela dei creditori, provocando ad essi un danno;
- procedere a formazione o aumento fittizio del capitale sociale, attribuendo azioni per un valore inferiore al loro valore nominale in sede di aumento del capitale sociale;
- porre in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, o che comunque ostacolino lo svolgimento dell'attività di controllo e di revisione da parte del socio e del Collegio Sindacale/Sindaco Unico;
- omettere di effettuare, con la dovuta completezza e tempestività, tutte le segnalazioni previste dalle leggi nei confronti delle Autorità Amministrative Indipendenti, nonché la trasmissione dei dati e documenti previsti dalla normativa e/o specificamente richiesti dalle stesse;

- esporre nelle predette comunicazioni e trasmissioni fatti non rispondenti al vero, ovvero occultare fatti rilevanti relativi alle condizioni economiche, patrimoniali o finanziarie di IIS CERT;
- porre in essere qualsiasi comportamento che sia di ostacolo all'esercizio delle funzioni delle Autorità Amministrative Indipendenti, anche in sede di ispezione (a titolo esemplificativo: espressa opposizione, rifiuti pretestuosi, o anche comportamenti ostruzionistici o di mancata collaborazione, quali ritardi nelle comunicazioni o nella messa a disposizione di documenti).

2.7.3. COMPORTAMENTI DA TENERE NELL'AMBITO DELLE ATTIVITÀ "SENSIBILI" RISPETTO AI REATI CON FINALITÀ DI TERRORISMO O DI EVERSIONE DELL'ORDINE DEMOCRATICO

Seppure l'analisi condotta sulle attività tipiche di IIS CERT porti a ritenere remoto il rischio connesso alla possibile verificazione di condotte idonee ad integrare i reati con finalità di terrorismo o di eversione dell'ordine democratico (in particolare, Funzione Acquisti e Funzione Commerciale), di cui all'art. 25 quater del Decreto, IIS CERT ha ravvisato l'opportunità di richiedere ai Destinatari di:

- effettuare una valutazione del "rischio paese": deve essere effettuata dai soggetti coinvolti una verifica preventiva per valutare il "rischio paese", ogniqualvolta IIS CERT intenda intraprendere iniziative economiche/commerciali in determinate aree geografiche ritenute a rischio terrorismo;
- verificare preventivamente, attraverso le informazioni disponibili, le controparti commerciali, fornitori, partner e consulenti, al fine di accertare la relativa rispettabilità e affidabilità prima di avviare rapporti d'affari, assicurando la tracciabilità e verificabilità delle verifiche effettuate;
- verifica del beneficiario di qualunque transazione finanziaria.

In caso di dubbi circa la corretta attuazione delle suddette regole comportamentali nel corso dello svolgimento delle attività operative, è fatto obbligo al soggetto interessato di interpellare il proprio responsabile ovvero di inoltrare richiesta di parere all'Organismo di Vigilanza.

Infine, nei confronti di terze parti contraenti (a titolo di esempio, collaboratori, consulenti, partner in affari, fornitori, ecc.) che operano con soggetti anche solo partecipati dalla Pubblica Amministrazione o coinvolte nello svolgimento di attività a rischio rispetto ai reati con finalità di terrorismo o di eversione dell'ordine democratico, per conto o nell'interesse di IIS CERT, i relativi contratti devono:

- essere definiti per iscritto, in tutte le loro condizioni e termini;

- contenere clausole standard che prevedano il rispetto dei principi etici e delle regole comportamentali sancite nel Codice Etico;
- prevedere apposite clausole risolutorie del rapporto contrattuale a fronte di violazioni dei principi etici di IIS CERT.

2.7.4. COMPORTAMENTI DA TENERE NELL'AMBITO DELLE ATTIVITÀ "SENSIBILI" RISPETTO AI REATI DI RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA INTRODOTTI DAL D. LGS. 231/2007

IIS CERT ha adottato delle regole comportamentali di carattere generale che si applicano ai Destinatari del presente Modello, che, a qualunque titolo sono designati o incaricati alla gestione del processo degli acquisti (es. materie prime, semilavorati, impianti e parti di impianti ecc.):

Alla luce di tali valutazioni, IIS CERT richiede ai Destinatari coinvolti nell'ambito delle attività sensibili sopra rappresentate di astenersi dal compiere ogni condotta che possa in qualsivoglia modo integrare direttamente o indirettamente le predette fattispecie di reato e/o agevolarne o favorirne la relativa commissione.

A tale proposito, si integrano le condotte del riciclaggio o dell'impiego di denaro, beni o altra utilità di provenienza illecita, quando si sostituisca o trasferisca denaro, beni o altra utilità di provenienza illecita ovvero si compiano operazioni atte ad ostacolare l'identificazione della loro provenienza illecita, mentre si integra la condotta della ricettazione allorquando si acquistino o ricevano ovvero occultino denaro o cose provenienti da un qualsiasi reato.

- utilizzare nelle transazioni il sistema bancario, richiedendo anche ai clienti che i pagamenti avvengano esclusivamente tramite tale sistema, che consente la tracciabilità dei trasferimenti finanziari;
- verificare, attraverso le informazioni disponibili, le controparti commerciali al fine di accertare la relativa rispettabilità e affidabilità prima di avviare con essi rapporti d'affari.

Tutti i Destinatari, nello svolgimento delle proprie funzioni e compiti aziendali, devono inoltre rispettare le norme riguardanti le limitazioni all'uso del contante e ai titoli al portatore previste dal D. Lgs. 231/2007, e successive modifiche e integrazioni.

A tale proposito, senza alcun intento esaustivo è fatto espresso divieto di:

- trasferire a qualsiasi titolo tra soggetti diversi, se non per il tramite di banche o istituti di moneta elettronica o Poste Italiane S.p.A., denaro contante o libretti di deposito bancari o postali al portatore o titoli al portatore in euro o in valuta estera, quando il valore dell'operazione, anche frazionata, sia complessivamente pari o superiore a Euro 2.500 o

alla diversa soglia che dovesse essere prevista da norme introdotte successivamente all'adozione del presente modello;

- di emettere assegni bancari e postali per importi pari o superiori a Euro 2.500 (o alla diversa soglia che dovesse essere prevista da norme introdotte successivamente all'adozione del presente modello) che non rechino l'indicazione del nome o della ragione sociale del beneficiario e la clausola di non trasferibilità;
- girare per l'incasso assegni bancari e postali emessi all'ordine del traente a soggetti diversi da banche o Poste Italiane S.p.A.

2.7.5. COMPORTAMENTI DA TENERE NELL'AMBITO DELLE ATTIVITÀ "SENSIBILI" RISPETTO AI REATI COLPOSI INTRODOTTI DALLA LEGGE 123/2007.

IIS CERT realizza in Italia l'attività sociale presso la sede ed inoltre presso siti di appartenenza dei clienti. IIS CERT risulta quindi potenzialmente esposto al rischio di verificazione di infortuni gravi (con prognosi superiore ai 40 giorni), con conseguente possibile chiamata dello stesso a rispondere a titolo di responsabilità amministrativa. Esso, di conseguenza, è particolarmente attento a promuovere la diffusione di una cultura della sicurezza e della consapevolezza dei rischi connessi alle attività lavorative svolte nel suo stabilimento, richiedendo, ad ogni livello, comportamenti responsabili e rispettosi delle procedure aziendali adottate in materia di sicurezza sul lavoro.

In via generale, è fatto obbligo a tutti i Destinatari, a vario titolo coinvolti nella gestione del sistema sicurezza adottato da IIS CERT nel sito produttivo, a tutela della sicurezza e salute dei dipendenti e di chiunque vi acceda, di dare attuazione, ciascuno per la parte di propria competenza e nel rispetto delle deleghe e procure attribuite da IIS CERT, nonché delle procedure aziendali vigenti in tale ambito, alle misure di prevenzione e di protezione predisposte a presidio dei rischi connessi alla sicurezza identificati nei Documenti di Valutazione dei Rischi (di seguito "DVR") relativi a ciascuna area aziendale.

In particolare per un'effettiva prevenzione dei rischi ed in conformità agli adempimenti prescritti dal D. Lgs. 81/2008, come successivamente modificato e integrato dal D. Lgs. 106/2009, nonché in coerenza con la ripartizione di ruoli, compiti e responsabilità in materia di sicurezza all'interno di IIS CERT e dei suoi stabilimenti, è fatta espressa richiesta:

- ai soggetti aziendali (a titolo di esempio, il Datore di Lavoro) e alle funzioni aziendali (a titolo di esempio, Funzione Tecnica, Funzione Risorse Umane ecc.) a vario titolo coinvolte nella gestione del sistema sicurezza, di svolgere i compiti loro attribuiti da IIS CERT in tale materia nel rispetto delle deleghe e procure conferite, nonché delle procedure aziendali

esistenti, avendo cura di informare e formare il personale che, nello svolgimento delle proprie attività, sia esposto a rischi connessi alla sicurezza;

- ai soggetti nominati da IIS CERT ai sensi del D. Lgs. 81/2008, come successivamente modificato e integrato dal D. Lgs. 106/2009 (es. il Responsabile del SPP, gli Addetti del Servizio di Prevenzione e Protezione; gli Incaricati dell'attuazione delle misure di prevenzione incendi, lotta antincendio, evacuazione dei lavoratori in caso di pericolo; gli addetti al Primo Soccorso; i Rappresentanti per la Sicurezza dei Lavoratori) di svolgere, ciascuno nell'ambito delle proprie competenze e attribuzioni, i compiti di sicurezza specificamente affidati dalla normativa vigente e previsti nel sistema sicurezza adottato da IIS CERT;
- ai preposti di vigilare sulla corretta osservanza, da parte di tutti i lavoratori delle misure e delle procedure di sicurezza adottate da IIS CERT, segnalando al Responsabile del SPP eventuali carenze o disallineamenti del sistema sicurezza, nonché comportamenti ad esso contrari;
- a tutti i dipendenti di aver cura della propria sicurezza e salute e di quella delle altre persone presenti sul luogo di lavoro, osservando le misure, le procedure di sicurezza e le istruzioni fornite da IIS CERT, nonché, per un'effettiva protezione dai rischi individuati, utilizzando obbligatoriamente, nello svolgimento delle proprie attività, i mezzi e i Dispositivi di Protezione Individuale consegnati da IIS CERT.

Ogni comportamento contrario al sistema sicurezza adottato da IIS CERT dovrà essere adeguatamente sanzionato, da parte di IIS CERT medesima, nell'ambito di un procedimento disciplinare conforme alle previsioni del contratto collettivo nazionale applicabile.

2.7.6. COMPORTAMENTI DA TENERE NELL'AMBITO DELLE ATTIVITÀ "SENSIBILI" RISPETTO AI REATI DI CRIMINALITÀ INFORMATICA (CYBERCRIME) INTRODOTTI DALLA L. 48/2008.

Le seguenti regole di comportamento di carattere generale si applicano ai Destinatari del presente Modello che, a qualunque titolo, sono designati o incaricati alla gestione e manutenzione dei server, delle banche dati, delle applicazioni, dei client e delle reti di telecomunicazione, nonché a tutti coloro che abbiano avuto assegnate password e chiavi di accesso al sistema informativo aziendale.

In particolare, coerentemente con le procedure di sicurezza del sistema informativo di IIS CERT, sono adottate le seguenti misure atte a mitigare il rischio di commissione delle fattispecie di reato previste dagli artt. 24 *bis* e 25 *novies* del D. Lgs. 231/2001:

- l'accesso alle informazioni che risiedono sui server e sulle banche dati aziendali, ivi inclusi i client, è limitato da strumenti di autenticazione;
- gli amministratori di sistema e gli addetti alla manutenzione sono muniti di credenziali di autenticazione;
- il personale dipendente è munito di univoche credenziali di autenticazione per l'accesso ai client;
- l'accesso alle applicazioni, da parte del personale IT, è garantito attraverso strumenti di autorizzazione;
- tutti i server e i laptop aziendali sono aggiornati periodicamente sulla base delle specifiche necessità;
- la rete di trasmissione dati aziendale è protetta da adeguati strumenti di limitazione degli accessi (firewall e proxy);
- tutti i server e i laptop aziendali sono protetti da programmi antivirus, aggiornati in modo automatico, contro il rischio di intrusione e l'azione di programmi di cui all'art. 615 quinquies del codice penale;
- il personale deve astenersi dal diffondere le informazioni ricevute da IIS CERT per l'uso dei mezzi informatici aziendali e l'accesso a dati, sistemi e applicazioni aziendali;
- il personale deve attuare i comportamenti richiesti da IIS CERT e necessari per proteggere il sistema informativo, diretti ad evitare che terzi possano accedervi in caso di allontanamento dalla postazione di lavoro;
- il personale deve accedere al sistema informativo aziendale unicamente attraverso i codici di identificazione assegnati, provvedendo alla modifica periodica;
- il personale deve astenersi da qualsiasi condotta (anche colposa) che possa compromettere la riservatezza e integrità delle informazioni e dei dati aziendali;
- il personale deve astenersi da qualsiasi condotta diretta a superare o aggirare le protezioni del sistema informativo aziendale o altrui;
- il personale deve conservare i codici identificativi assegnati, astenendosi dal comunicarli a terzi che in tal modo potrebbero accedere abusivamente a dati aziendali riservati;
- il personale deve astenersi dall'installare programmi senza aver preventivamente informato la funzione aziendale preposta alla gestione della sicurezza informatica;

- il personale non può duplicare e/o diffondere in qualsiasi forma programmi e files se non nelle forme e per gli scopi di servizio per i quali sono stati assegnati;
- il personale deve astenersi dal riprodurre CD, DVD e più in generale supporti sottoposti a licenza d'uso, in quanto questa rientra tra le attività regolamentate dalla L.22 aprile 1941, n.633 "Protezione del diritto d'autore e di altri diritti connessi al suo esercizio" così come modificata dalla L.18 agosto 2000, n.248, pertanto il personale CED non è autorizzato a riprodurre tali supporti;
- il personale deve astenersi dall'utilizzo di connessioni alternative rispetto a quelle fornite da IIS CERT nell'espletamento dell'attività lavorativa resa in suo favore;
- il personale deve astenersi dall'utilizzo improprio dei supporti informatici aziendali, compresi quelli portatili;
- il personale deve astenersi dall'utilizzo della rete aziendale tramite supporti informatici non aziendali;
- il personale deve attenersi ad un corretto utilizzo degli indirizzi di posta elettronica certificata "PEC", secondo quanto stabilito da apposite istruzioni.

2.7.7. COMPORTAMENTI DA TENERE NELL'AMBITO DELLE ATTIVITÀ "SENSIBILI" RISPETTO AI DELITTI CONTRO L'INDUSTRIA E IL COMMERCIO INTRODOTTI DALLA LEGGE 99/2009

Le seguenti regole di comportamento di carattere generale si applicano ai Destinatari del presente Modello che, a qualunque titolo, sono designati o incaricati della gestione e commercializzazione dei prodotti.

In particolare, sono adottate le seguenti misure atte a mitigare il rischio di commissione delle fattispecie di reato previste dall'art. 25 bis-1 del D. Lgs. 231/2001:

- predisposizione di idonee procedure di controllo attraverso l'inserimento di clausole contrattuali con i fornitori che prevedano la garanzia da parte degli stessi di non ledere, nell'ambito dell'attività svolta, i diritti dei terzi (ad esempio: consumatori);
- inserimento di clausole contrattuali con i fornitori che prevedano la responsabilità di quest'ultimi anche per l'operato di eventuali sub-fornitori;
- controlli sulla qualità, provenienza, caratteristiche e origine dei prodotti oggetto di successiva commercializzazione.

SEZIONE TERZA

3. ORGANISMO DI VIGILANZA

3.1. PREMESSA

L'art. 6, comma 1, del D. Lgs. 231/2001 prevede che la funzione di vigilare e di curare l'aggiornamento del Modello sia affidata ad un Organismo di Vigilanza interno all'ente che, dotato di autonomi poteri di iniziativa e di controllo, eserciti in via continuativa i compiti ad esso rimessi.

A tale proposito, le Linee Guida di Confindustria evidenziano che, sebbene il D. Lgs. 231/2001 consenta di optare per una composizione sia monocratica che plurisoggettiva, la scelta tra l'una o l'altra soluzione deve tenere conto delle finalità perseguite dalla legge e, quindi, assicurare l'effettività dei controlli in relazione alla dimensione e complessità organizzativa dell'ente.

Non potrà essere nominato componente dell'Organismo di Vigilanza, e, se nominato decade, l'interdetto, l'inabilitato, il fallito o chi è stato condannato, ancorché con condanna non definitiva, ad una pena che importi l'interdizione, anche temporanea, dai pubblici uffici o l'incapacità ad esercitare uffici direttivi ovvero sia stato condannato, anche con sentenza non definitiva o con sentenza di patteggiamento, per aver commesso uno dei reati previsti dal D. Lgs. 231/2001.

Il Decreto richiede, inoltre, che l'Organismo di Vigilanza svolga le sue funzioni al di fuori dei processi operativi dell'ente e che sia collocato in posizione di staff al Consiglio di Amministrazione, svincolato da ogni rapporto gerarchico con i singoli responsabili delle funzioni/direzioni aziendali.

In caso di nomina di un componente esterno, lo stesso non dovrà avere rapporti commerciali con l'ente che possano configurare ipotesi di conflitto di interessi e che possano comprometterne l'indipendenza di giudizio.

In ossequio alle prescrizioni del D. Lgs. 231/2001, alle indicazioni espresse dalle Linee Guida di Confindustria e agli orientamenti della giurisprudenza formatisi in materia, IIS CERT ha ritenuto di istituire un organo collegiale, che, per la composizione scelta, possa assicurare autorevolezza, indipendenza e credibilità dello svolgimento delle relative funzioni.

L'Organismo di Vigilanza è stato definito in modo da poter garantire i seguenti requisiti:

- *Autonomia e indipendenza*: detto requisito è assicurato dall'assenza di riporto gerarchico all'interno dell'organizzazione e dalla facoltà di reporting al massimo vertice aziendale.
- *Professionalità*: requisito questo garantito dal bagaglio di conoscenze professionali, tecniche e pratiche, di cui dispongono i componenti dell'Organismo di Vigilanza.
- *Continuità d'azione*: con riferimento a tale requisito, l'Organismo di Vigilanza è tenuto a vigilare costantemente, attraverso poteri di indagine, sul rispetto del Modello, a curarne l'attuazione e l'aggiornamento, rappresentando un riferimento costante per tutto il personale di IIS CERT.

L'Organismo di Vigilanza è istituito con l'approvazione del presente Modello. I suoi componenti sono nominati dal Consiglio di Amministrazione secondo le indicazioni del Socio Unico e restano in carica per 3 anni e sono in ogni caso rieleggibili.

Mediante l'approvazione del presente atto sono riconosciuti al suddetto Organismo i poteri e le funzioni di cui ai successivi paragrafi 3.2, 3.3 e 3.4. È inoltre conferito all'Organismo il potere di dotarsi di un proprio regolamento e di approvare uno schema descrittivo dei flussi informativi da e verso di sé.

All'Organismo di Vigilanza è riconosciuto annualmente un *budget* di spesa adeguato per lo svolgimento delle relative funzioni. L'Organismo delibera in autonomia le spese da sostenere e, in caso di spese eccedenti il *budget* approvato, dovrà essere autorizzato direttamente dal Consiglio di Amministrazione, sentito il Socio Unico.

La revoca dei membri dell'Organismo di Vigilanza potrà avvenire esclusivamente per giusta causa e previa delibera del Consiglio di Amministrazione di IIS CERT, sentito il Socio Unico.

3.2. POTERI E FUNZIONI DELL'ORGANISMO DI VIGILANZA

All'Organismo di Vigilanza sono affidati i seguenti compiti:

- vigilare sul funzionamento e osservanza del Modello;
- curarne l'aggiornamento.

Tali compiti sono svolti dall'Organismo attraverso le seguenti attività:

- vigilanza sulla diffusione nel contesto aziendale della conoscenza, della comprensione e dell'osservanza del Modello;
- vigilanza sulla validità ed adeguatezza del Modello, con particolare riferimento ai comportamenti riscontrati nel contesto aziendale;

- verifica dell'effettiva capacità del Modello di prevenire la commissione dei reati previsti dal D. Lgs. 231/2001;
- proposte di aggiornamento del Modello nell'ipotesi in cui si renda necessario e/o opportuno effettuare correzioni e/o adeguamenti dello stesso, in relazione alle mutate condizioni legislative e/o aziendali;
- comunicazione su base continuativa al Consiglio di Amministrazione in ordine alle attività svolte;
- comunicazioni periodiche al Collegio Sindacale/Sindaco Unico su richiesta dello stesso in ordine alle attività svolte;
- occasionalmente nei confronti del Socio Unico e del Collegio Sindacale/Sindaco Unico, nei casi di presunte violazioni poste in essere dai vertici aziendali o dai Consiglieri di Amministrazione, potendo ricevere da detti organi richieste di informazioni o di chiarimenti.

Nello svolgimento di dette attività, l'Organismo provvederà ai seguenti adempimenti:

- elaborare un piano periodico di formazione volto a favorire la conoscenza delle prescrizioni del Modello di IIS CERT, differenziato secondo il ruolo e la responsabilità dei destinatari;
- istituire specifici canali informativi "dedicati" (indirizzo di posta elettronica dedicato), diretti a facilitare il flusso di segnalazioni ed informazioni verso l'Organismo;
- raccogliere, elaborare, conservare e aggiornare ogni informazione rilevante ai fini della verifica dell'osservanza del Modello;
- verificare e controllare periodicamente le aree/operazioni a rischio individuate nel Modello;
- verificare che le violazioni del Modello siano effettivamente e adeguatamente sanzionate da IIS CERT;
- segnalare tempestivamente al Consiglio di Amministrazione, nella persona del Presidente e con i mezzi ritenuti più idonei allo scopo, le presunte violazioni del Modello che abbiano parvenza di fondatezza, laddove le stesse possano coinvolgere la responsabilità di IIS CERT in quanto poste in essere da soggetti in posizioni apicali e da dipendenti con qualifica dirigenziale, di cui sia venuto a conoscenza per mezzo di segnalazione o che abbia accertato esso stesso.

Al fine di consentire all'Organismo la miglior conoscenza in ordine all'attuazione del Modello, alla sua efficacia e al suo effettivo funzionamento, nonché alle esigenze di aggiornamento dello

stesso, è fondamentale che l'Organismo di Vigilanza operi in stretta collaborazione con le Direzioni aziendali.

Ai fini dello svolgimento degli adempimenti sopra elencati, l'Organismo è dotato dei poteri di seguito indicati:

- accedere liberamente, senza autorizzazioni preventive, a ogni documento aziendale rilevante per lo svolgimento delle funzioni attribuite all'Organismo ai sensi del D. Lgs. 231/2001;
- emanare regolamenti, disposizioni e ordini di servizio intesi a regolare la propria attività;
- disporre che i responsabili delle Funzioni aziendali, e in ogni caso tutti i Destinatari, forniscano tempestivamente le informazioni, i dati e/o le notizie loro richieste per individuare aspetti connessi alle varie attività aziendali rilevanti ai sensi del Modello e per la verifica dell'effettiva attuazione dello stesso da parte delle strutture organizzative aziendali;
- ricorrere a consulenti esterni 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.

Per un miglior svolgimento delle proprie attività, l'Organismo potrà delegare uno o più compiti specifici ai singoli suoi componenti, che li svolgeranno in nome e per conto dell'Organismo stesso. In ordine ai compiti delegati dall'Organismo a singoli membri dello stesso, la responsabilità da essi derivante ricade sull'Organismo nel suo complesso.

3.3. REPORTING DELL'ORGANISMO DI VIGILANZA

Come sopra già anticipato, al fine di garantire la piena autonomia e indipendenza nello svolgimento delle relative funzioni, l'Organismo di Vigilanza comunica direttamente e continuativamente al Consiglio di Amministrazione di IIS CERT, e, periodicamente, al Socio Unico ed al Collegio Sindacale/Sindaco Unico.

Il riporto a siffatti organi sociali, costituisce anche la miglior garanzia del controllo ultimo sull'operato degli amministratori, affidato - per previsione legislativa e statutaria - al socio.

Segnatamente, l'Organismo di Vigilanza riferisce a tali organi lo stato di fatto sull'attuazione del Modello, gli esiti dell'attività di vigilanza svolta e gli eventuali interventi opportuni per l'implementazione del Modello:

- in modo continuativo nei confronti del Consiglio di Amministrazione;

- almeno annualmente, al Socio Unico ed al Consiglio di Amministrazione attraverso una relazione scritta nella quale vengono illustrate le attività di monitoraggio svolte, le criticità emerse e gli eventuali interventi correttivi o migliorativi ritenuti opportuni;
- nei confronti del Collegio Sindacale/Sindaco Unico, su richiesta dello stesso in ordine alle attività svolte;
- occasionalmente nei confronti del Socio Unico e del Collegio Sindacale/Sindaco Unico, nei casi di presunte violazioni poste in essere dai vertici aziendali o dai Consiglieri di Amministrazione, potendo ricevere da detti organi richieste di informazioni o di chiarimenti.

L'Organismo di Vigilanza potrà essere convocato in qualsiasi momento e, al contempo, potrà – a sua volta – richiedere al Consiglio di Amministrazione di IIS CERT di essere convocato ogni volta che ravveda l'opportunità di un esame o di un intervento in materie inerenti il funzionamento e l'efficace attuazione del Modello o in relazione a situazioni specifiche.

A garanzia di un corretto ed efficace flusso informativo, l'Organismo ha inoltre la possibilità, al fine di un pieno e corretto esercizio dei suoi compiti, di richiedere chiarimenti o informazioni direttamente ai soggetti aventi le principali responsabilità operative.

3.4. FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA

Il D. Lgs. 231/2001 enuncia, tra le esigenze che il Modello deve soddisfare, l'istituzione di obblighi informativi nei confronti dell'Organismo di Vigilanza, diretti a consentire all'Organismo stesso lo svolgimento delle proprie attività di vigilanza e di verifica sulle aree ritenute dall'ente a rischio di reato.

A tale proposito devono essere comunicati all'Organismo di Vigilanza le seguenti informazioni:

- su base periodica, le informazioni, dati, notizie e documenti previamente identificati dall'Organismo di Vigilanza secondo le modalità e le tempistiche definite dall'Organismo medesimo;
- su base occasionale, ogni altra informazione, di qualsivoglia natura, attinente l'attuazione del Modello nell'area di attività ritenuta da IIS CERT a rischio di reato (c.d. segnalazioni).

Sono stati, pertanto, istituiti precisi obblighi gravanti sugli organi sociali e sul personale di IIS CERT.

In particolare, gli organi sociali devono riferire all'Organismo di Vigilanza ogni informazione rilevante per il rispetto e il funzionamento del Modello.

I Destinatari devono riferire all'Organismo di Vigilanza ogni informazione relativa a comportamenti che possano integrare violazioni delle prescrizioni del Modello o fattispecie di reato.

A tali fini è istituito un canale di comunicazione per la consultazione dell'Organismo di Vigilanza, consistente in un indirizzo di posta elettronica dedicato al quale potranno essere inviate le eventuali segnalazioni.

Tale modalità di trasmissione delle segnalazioni sono volte a garantire la riservatezza dei segnalanti anche al fine di evitare atteggiamenti ritorsivi nel loro confronti.

L'Organismo di Vigilanza valuterà le segnalazioni pervenutegli, e potrà convocare, qualora lo ritenga opportuno, sia il segnalante per ottenere maggiori informazioni, assicurandogli la necessaria riservatezza, che il presunto autore della violazione, dando inoltre luogo a tutti gli accertamenti e le indagini che siano necessarie per appurare la fondatezza della segnalazione.

Le segnalazioni anonime non sono ammesse e, di conseguenza, non verranno prese in considerazione.

Nel caso in cui le segnalazioni ricevute dall'Organismo dovessero riguardare la violazione del Modello da parte di un dipendente con qualifica dirigenziale o di altro soggetto apicale, il Presidente dell'Organismo, pervenuta la segnalazione, informerà senza indugio e nelle forme ritenute più idonee il Consiglio di Amministrazione di IIS CERT, ovvero il Presidente, che riferirà al Consiglio medesimo.

Oltre alle segnalazioni sopra indicate, devono essere obbligatoriamente trasmesse all'Organismo di Vigilanza le informazioni concernenti:

- provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, anche amministrativa, che vedano il coinvolgimento di IIS CERT o di soggetti apicali, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i reati di cui al D. Lgs. 231/2001, fatti salvi gli obblighi di riservatezza e segretezza legalmente imposti;
- richieste di assistenza legale inoltrate dai dirigenti e/o dai dipendenti in caso di avvio di procedimento giudiziario, in particolare per i reati ricompresi nel D. Lgs. 231/2001;
- attività di controllo svolte dai responsabili di altre Funzioni aziendali dalle quali siano emersi fatti, atti, eventi od omissioni con profili di criticità rispetto all'osservanza delle norme del D. Lgs. 231/2001 o del Modello;

- modifiche nel sistema delle deleghe e delle procure, modifiche statutarie o modifiche dell'organigramma aziendale;
- notizie relative all'effettiva attuazione, a tutti i livelli aziendali, del Modello, con evidenza dei procedimenti disciplinari svolti e delle eventuali sanzioni irrogate (ivi compresi i provvedimenti verso i dipendenti), ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni;
- segnalazione di infortuni gravi (omicidio colposo o lesioni colpose gravi o gravissime, in ogni caso qualsiasi infortunio con prognosi superiore ai 40 giorni) occorsi a dipendenti, addetti alla manutenzione, appaltatori e/o collaboratori presenti nei luoghi di lavoro di IIS CERT e, più in generale, chiunque acceda agli stessi.

Nell'esercizio del proprio potere ispettivo, l'Organismo di Vigilanza può accedere liberamente a tutte le fonti di informazione di IIS CERT, nonché prendere visione di qualsiasi documento di quest'ultima e consultare dati relativi alla stessa.

Tutte le informazioni, la documentazione e le segnalazioni raccolte nell'espletamento dei compiti istituzionali devono essere archiviate e custodite dall'Organismo di Vigilanza, avendo cura di mantenere riservati i documenti e le informazioni acquisite, anche nel rispetto della normativa sulla privacy.

SEZIONE QUARTA

4. SISTEMA SANZIONATORIO

4.1. DESTINATARI E APPARATO SANZIONATORIO E/O RISOLUTIVO

La definizione di un sistema sanzionatorio, applicabile in caso di violazione delle disposizioni del presente Modello e dei principi del Codice Etico, costituisce condizione necessaria per garantire l'efficace attuazione del Modello stesso, nonché presupposto imprescindibile per consentire a IIS CERT di beneficiare dell'esimente dalla responsabilità amministrativa.

L'applicazione delle sanzioni disciplinari prescinde dall'instaurazione e dagli esiti di un procedimento penale eventualmente avviato nei casi in cui la violazione integri un'ipotesi di reato rilevante ai sensi del D. Lgs. 231/2001.

Le sanzioni comminabili sono diversificate in ragione della natura del rapporto tra l'autore della violazione e IIS CERT, nonché del rilievo e gravità della violazione commessa e del ruolo e responsabilità dell'autore.

In generale, le violazioni possono essere classificate nei seguenti comportamenti:

- comportamenti che integrano una mancata attuazione colposa delle prescrizioni del Modello, ivi comprese direttive, procedure o istruzioni aziendali;
- comportamenti che integrano una grave trasgressione dolosa delle prescrizioni del Modello, ivi comprese direttive, procedure o istruzioni di IIS CERT, tale da compromettere il rapporto di fiducia tra l'autore e IIS CERT in quanto preordinata in modo univoco a commettere un reato.

4.1.1. SANZIONI PER IL PERSONALE DIPENDENTE

In relazione al personale dipendente, IIS CERT deve rispettare i limiti di cui all'art. 7 della Legge 300/1970 (c.d. Statuto dei lavoratori) e le previsioni contenute nei contratti vigente tra IIS CERT e i suoi dipendenti (Contratto Collettivo nazionale di lavoro per i dipendenti non dirigenti del Gruppo IIS e Contratto Collettivo Nazionale di Lavoro per i dirigenti di aziende produttrici di beni e servizi), sia con riguardo alle sanzioni comminabili che alle modalità di esercizio del potere disciplinare.

L'inosservanza delle procedure e delle disposizioni indicate nel Modello adottato ai sensi del D. Lgs. 231/2001, nonché le violazioni delle disposizioni e dei principi stabiliti nel Codice Etico da

parte del personale dipendente costituisce inadempimento alle obbligazioni derivanti dal rapporto di lavoro ex art. 2104 c.c. e illecito disciplinare.

Più in particolare, l'adozione, da parte di un dipendente di IIS CERT, di un comportamento qualificabile, in base a quanto indicato al comma precedente, come illecito disciplinare, costituisce inoltre violazione dell'obbligo dei lavoratori di eseguire con la massima diligenza i compiti loro affidati, attenendosi alle direttive di IIS CERT, così come previsto nei contratti vigente tra IIS CERT e i suoi dipendenti (Contratto Collettivo nazionale di lavoro per i dipendenti non dirigenti del Gruppo IIS e Contratto Collettivo Nazionale di Lavoro per i dirigenti di aziende produttrici di beni e servizi).

Con riferimento alle sanzioni irrogabili, esse verranno applicate nel rispetto delle procedure previste dai contratti vigenti applicabili.

Al personale dipendente possono essere comminate le seguenti sanzioni:

- richiamo verbale;
- ammonizione scritta;
- multa;
- sospensione dal lavoro;
- licenziamento.

Tali sanzioni saranno comminate dall'Amministratore Delegato, sulla base del rilievo che assumono le singole fattispecie considerate e saranno proporzionate a seconda della loro gravità.

Al fine di esplicitare preventivamente i criteri di correlazione tra le violazioni dei lavoratori ed i provvedimenti disciplinari adottati, si prevede che:

- Incorre nei provvedimenti disciplinari conservativi il lavoratore che violi le procedure interne o tenga un comportamento non conforme alle prescrizioni del Codice Etico (ad es. che non osservi le procedure prescritte, ometta di dare comunicazione all'Organismo di Vigilanza delle informazioni prescritte, ometta di svolgere controlli, ecc.) o adotti, nell'espletamento di attività nelle aree a rischio, un comportamento non conforme alle prescrizioni contenute nel Modello stesso, dovendosi ravvisare in tali comportamenti una non esecuzione degli ordini impartiti da IIS CERT sia in forma scritta che verbale.
- Incorre, inoltre, nei provvedimenti disciplinari risolutivi il lavoratore che:

- adotti, nell'espletamento delle attività nelle aree a rischio, un comportamento non conforme alle prescrizioni contenute nel Modello e nel Codice Etico, diretto in modo univoco alla commissione di un reato sanzionato dal D. Lgs. 231/2001, dovendosi ravvisare in tale comportamento un'infrazione alla disciplina e alla diligenza nel lavoro, talmente grave da far venire meno la fiducia dell'azienda nei confronti del lavoratore;
- adotti, nell'espletamento delle attività nelle aree a rischio, un comportamento che si ponga palesemente in contrasto con le prescrizioni contenute nel Modello e nel Codice Etico, tale da determinare la concreta applicazione a carico di IIS CERT delle misure previste dal D. Lgs. 231/2001, dovendosi ravvisare in tale comportamento un atto che provoca a IIS CERT grave nocumento morale e materiale che non consente la prosecuzione del rapporto, neppure in via temporanea.

IIS CERT non potrà adottare alcun provvedimento disciplinare nei confronti del dipendente senza avergli preventivamente contestato l'addebito e senza averlo sentito a sua difesa. Salvo che per il richiamo verbale, la contestazione dovrà essere effettuata per iscritto ed i provvedimenti disciplinari non potranno esser comminati prima che siano trascorsi cinque giorni, nel corso dei quali il lavoratore potrà presentare le sue giustificazioni.

Se il provvedimento non verrà comminato entro i sei giorni successivi a tali giustificazioni, queste si riterranno accolte.

Il lavoratore potrà presentare le proprie giustificazioni anche verbalmente, con l'eventuale assistenza di un rappresentante dell'Associazione sindacale cui aderisce.

La comminazione del provvedimento dovrà essere motivata e comunicata per iscritto.

I provvedimenti disciplinari potranno essere impugnati dal lavoratore in sede sindacale, secondo le norme contrattuali relative alle vertenze. Il licenziamento potrà essere impugnato secondo le procedure previste dall'art. 7 della Legge n. 604 del 15 luglio 1966, confermate dall'articolo 18 della Legge n. 300 del 20 maggio 1970.

Non si terrà conto a nessun effetto dei provvedimenti disciplinari decorsi due anni dalla loro comminazione.

Il tipo e l'entità di ciascuna delle sanzioni sopra elencate saranno determinate in relazione:

- alla gravità della violazione commessa;
- alla mansione, ruolo, responsabilità e autonomia del dipendente;
- alla prevedibilità dell'evento;

- all'intenzionalità del comportamento o grado di negligenza, imprudenza o imperizia;
- al comportamento complessivo dell'autore della violazione, con riguardo alla sussistenza o meno di precedenti disciplinari;
- ad altre particolari circostanze che caratterizzino la violazione.

Le sanzioni disciplinari (così come previsto dall'art. 7 L. 300/70) ed il Codice Etico, sono portate a conoscenza del lavoratore mediante affissione in luogo accessibile a tutti.

4.1.2. SANZIONI PER COLLABORATORI SOTTOPOSTI A DIREZIONE O VIGILANZA

L'inosservanza delle procedure indicate nel Modello adottato da IIS CERT ai sensi del D. Lgs. 231/2001, nonché le violazioni delle disposizioni e dei principi stabiliti nel Codice Etico da parte dei collaboratori sottoposti a direzione o vigilanza di IIS CERT, potrà determinare, in conformità a quanto disciplinato nello specifico rapporto contrattuale, la risoluzione del relativo contratto, ovvero il diritto di recesso dal medesimo, ferma restando la facoltà di richiedere il risarcimento dei danni verificatisi in conseguenza di detti comportamenti, ivi inclusi i danni causati dall'applicazione da parte del giudice delle misure previste dal D. Lgs. 231/2001.

Tali sanzioni saranno adottate dall'Amministratore Delegato.

4.1.3. SANZIONI PER I LAVORATORI SUBORDINATI CON LA QUALIFICA DI DIRIGENTI

La violazione delle norme di legge, delle disposizioni del Codice Etico e delle prescrizioni previste dal presente Modello commesse da dirigenti, ivi inclusa la violazione degli obblighi di informazione nei confronti dell'Organismo di Vigilanza, nonché, in generale, l'assunzione di comportamenti idonei ad esporre a IIS CERT all'applicazione di sanzioni amministrative previste dal D. Lgs. 231/2001, potranno determinare l'applicazione delle sanzioni di cui alla contrattazione collettiva per le altre categorie di dipendenti, nel rispetto degli artt. 2106, 2118 e 2119 cod. civ., nonché dell'art. 7 Legge 300/1970.

In via generale, al personale dirigente possono essere comminate le seguenti sanzioni:

- multa;
- sospensione dal lavoro;
- risoluzione anticipata dal rapporto di lavoro.

L'accertamento di eventuali violazioni, nonché dell'inadeguata vigilanza e della mancata tempestiva informazione all'Organismo di Vigilanza, potranno determinare a carico dei lavoratori con qualifica dirigenziale, la sospensione a titolo cautelare dalla prestazione lavorativa, fermo il diritto del dirigente alla retribuzione, nonché, sempre in via provvisoria e

cautelare per un periodo non superiore a tre mesi, l'assegnazione ad incarichi diversi nel rispetto dell'art. 2103 cod. civ.

Nei casi di gravi violazioni, IIS CERT potrà procedere alla risoluzione anticipata del contratto di lavoro senza preavviso ai sensi e per gli effetti dell'art. 2119 cod. civ.

Tali sanzioni saranno adottate dal Consiglio di Amministrazione.

4.1.4. MISURE NEI CONFRONTI DEGLI AMMINISTRATORI

In caso di violazione accertata del Modello o del Codice Etico da parte degli Amministratori, l'Organismo di Vigilanza informerà tempestivamente l'intero Consiglio di Amministrazione, il Socio Unico e il Collegio Sindacale/Sindaco Unico di IIS CERT affinché provvedano ad assumere o promuovere le iniziative più opportune ed adeguate, in relazione alla gravità della violazione rilevata e conformemente ai poteri previsti dalla vigente normativa e dallo Statuto.

In particolare, in caso di violazioni del Modello o del Codice Etico di lieve entità (non diretta in modo univoco ad agevolare o commettere un reato ricompreso nel Decreto) da parte di uno o più Amministratori, il Consiglio di Amministrazione potrà procedere direttamente all'irrogazione della misura sanzionatoria del richiamo formale scritto o della revoca temporanea delle procure.

In caso invece di violazioni del Modello o del Codice Etico da parte di uno o più Amministratori di particolare rilevanza in quanto dirette in modo univoco ad agevolare ovvero a commettere un reato rilevante ai sensi del D. Lgs. 231/2001, le misure sanzionatorie (quali a mero titolo di esempio, la sospensione temporanea dalla carica e, nei casi più gravi, la revoca dalla stessa) saranno adottate dal Socio Unico, sentito il Collegio Sindacale/Sindaco Unico.

4.1.5. MISURE NEI CONFRONTI DEGLI APICALI

In ogni caso, anche la violazione dello specifico obbligo di vigilanza dei sottoposti gravante sugli apicali comporterà, da parte di IIS CERT, l'assunzione delle misure sanzionatorie ritenute più opportune in relazione, da una parte, alla natura e gravità della violazione commessa e, dall'altra, alla qualifica del medesimo apicale che dovesse commettere la violazione.

4.1.6. SOGGETTI AVENTI RAPPORTI CONTRATTUALI/COMMERCIALI

La violazione delle disposizioni e dei principi stabiliti nel Codice Etico da parte dei soggetti aventi rapporti contrattuali, commerciali o accordi di partnership con IIS CERT, potrà determinare, in conformità a quanto disciplinato nello specifico rapporto contrattuale, la risoluzione del relativo contratto, ovvero il diritto di recesso dal medesimo fermo restando la facoltà di richiedere il risarcimento dei danni verificatisi in conseguenza di detti comportamenti, ivi inclusi i danni causati dall'applicazione da parte del giudice delle misure previste dal D. Lgs. 231/2001.

5. INFORMAZIONE E FORMAZIONE DEL PERSONALE

Conformemente a quanto previsto dal D. Lgs. 231/2001, IIS CERT ha definito un programma di comunicazione e formazione finalizzato a garantire una corretta divulgazione e conoscenza del Modello e delle regole di condotta in esso contenute, nei confronti delle risorse già presenti in azienda e di quelle da inserire, con differente grado di approfondimento in ragione del diverso livello di coinvolgimento delle stesse nelle attività a rischio.

Il sistema di informazione e formazione è supervisionato ed integrato dall'Organismo di Vigilanza, in collaborazione con la Funzione Risorse Umane e con i responsabili delle Funzioni aziendali di volta in volta coinvolte nell'applicazione del Modello.

In relazione alla comunicazione del Modello, IIS CERT si impegna a:

- diffondere il Modello nel contesto aziendale attraverso la pubblicazione sul sito web aziendale e/o con qualsiasi altro strumento ritenuto idoneo;
- predisporre una newsletter destinata a tutto il personale avente qualifica di impiegato, quadro o dirigente;
- organizzare uno specifico incontro formativo nell'ambito del quale illustrare il D. Lgs. 231/2001 ed il Modello adottato.

In ogni caso, l'attività di formazione finalizzata a diffondere la conoscenza della normativa di cui al D. Lgs. 231/2001 e le prescrizioni del Modello adottato sarà differenziata nei contenuti e nelle modalità in funzione della qualifica dei destinatari, del livello di rischio dell'area in cui operano, dell'avere o meno funzioni di rappresentanza di IIS CERT.

Le attività di comunicazione iniziale e di formazione periodica al personale aziendale sarà documentata a cura dell'Organismo di Vigilanza.

6. AGGIORNAMENTO DEL MODELLO

L'adozione di eventuali aggiornamenti del Modello compete al Consiglio di Amministrazione, che lo eserciterà mediante delibera con le modalità previste per la sua adozione, sentito previamente il Socio Unico.

L'attività di aggiornamento, intesa sia come integrazione sia come modifica, è volta a garantire l'adeguatezza e l'idoneità del Modello, valutate rispetto alla funzione preventiva di commissione dei reati previsti dal D. Lgs. 231/2001.

Compete, invece, all'Organismo di Vigilanza la concreta verifica circa la necessità od opportunità di procedere all'aggiornamento del Modello, facendosi promotore di tale esigenza nei confronti del Consiglio di Amministrazione e del Socio Unico.