



Modello di organizzazione, gestione e controllo – aggiornamento 2016
ex decreto legislativo 8 giugno 2001, n. 231

PARTE SPECIALE

Modello di organizzazione, gestione e controllo

Ex D.Lgs. 231/01 integrato con l'art. 30 D.Lgs. 81/08 e la L. 190/12

M.O.G. VEGA - Aggiornamento 2016

Modello aggiornato approvato con Delibera del Consiglio di Amministrazione del 21/03/2017



Modello di organizzazione, gestione e controllo – aggiornamento 2016
ex decreto legislativo 8 giugno 2001, n. 231

INDICE

REATI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE	3
DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI.....	12
DELITTI DI CRIMINALITA' ORGANIZZATA	20
REATI SOCIETARI.....	26
REATI DI OMICIDIO COLPOSO E LESIONI COLPOSE GRAVI O GRAVISSIME, COMMESSI CON VIOLAZIONI DELLE NORMA ANTINFORTUNISTICHE E SULLA TUTELA DELL'IGIENE E DELLA SALUTE SUL LAVORO.....	34
RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA.....	47
REATI AMBIENTALI	53



*Modello di organizzazione, gestione e controllo – aggiornamento 2016
ex decreto legislativo 8 giugno 2001, n. 231*

REATI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE

(ART. 24 E ART 25)

1. LA TIPOLOGIA DEI REATI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE (ARTT. 24 E 25 DEL DECRETO)

Per quanto concerne la presente Parte Speciale, si provvede di seguito ad elencare i reati contemplati negli artt. 24 e 25 del Decreto.

- Art. 316-bis c.p. - Malversazione a danno dello Stato, di altro ente pubblico o delle Comunità Europee
- Art. 316-ter c.p.- Indebita percezione di erogazioni pubbliche
- Art. 317 c.p. - Concussione
- Art. 318 – 319-320 c.p.- Corruzione per un atto d'ufficio o contrario ai doveri d'ufficio
- Art. 321 c.p.- Sanzioni per il corruttore
- Art. 322 c.p. -Istigazione alla corruzione
- Art. 322-bis c.p. - Peculato, concussione, corruzione e istigazione alla corruzione di membri degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri
- Art. 640, comma 2 n. 1 c.p. Truffa in danno dello Stato, di altro ente pubblico o dell'Unione Europea
- Art. 640-bis c.p. - Truffa aggravata per il conseguimento di erogazioni pubbliche
- Art. 640-ter c.p. -Frode informatica in danno dello Stato o di altro ente pubblico

2. LE AREE DI ATTIVITA' A RISCHIO

I reati sopra considerati hanno come presupposto l'instaurazione di rapporti con la Pubblica Amministrazione (intesa in senso lato) e lo svolgimento di attività concretanti una pubblica funzione o un pubblico servizio.



Tenuto conto, peraltro, della molteplicità dei rapporti che VEGA intrattiene con le Amministrazioni Pubbliche o con soggetti che svolgono una pubblica funzione od un pubblico servizio sono state ritenute specificamente a rischio le seguenti aree di attività:

1. Gestione dei rapporti con soggetti pubblici per l'ottenimento di autorizzazioni e licenze, per l'esercizio delle attività aziendali;
2. Gestione dei rapporti con i soggetti pubblici per gli aspetti che riguardano la sicurezza e l'igiene sul lavoro (d.lgs. n. 81 del 2008) e il rispetto delle cautele previste da leggi e regolamenti per l'impiego di dipendenti adibiti a particolari mansioni;
3. Gestione dei rapporti con i soggetti pubblici relativi all'assunzione di personale anche con riferimento alle categorie protette o la cui assunzione è agevolata;
4. Gestione di trattamenti previdenziali del personale e/o gestione dei relativi accertamenti/ispezioni;
5. Gestione dei rapporti con organismi di vigilanza relativi allo svolgimento di attività regolate dalla legge;
6. Gestione delle attività di richiesta/acquisizione e/o gestione di contributi, sovvenzioni, finanziamenti, assicurazioni o garanzie concesse da soggetti pubblici;
7. Predisposizione di dichiarazioni dei redditi o dei sostituti di imposta o di altre dichiarazioni funzionali alla liquidazione di tributi in genere;
8. Adempimenti presso soggetti pubblici, quali comunicazioni, dichiarazioni, deposito atti e documenti, pratiche, ecc, differenti da quelli descritti ai precedenti punti e nelle verifiche/accertamenti/procedimenti sanzionatori che ne derivano;
9. Gestione di procedimenti giudiziari o arbitrali;

Per ognuna delle citate aree di attività ritenute a rischio sono stati identificati i processi aziendali e i controlli per ridurre il rischio dei comportamenti illeciti.



3. DESTINATARI DELLA PARTE SPECIALE

La presente Parte Speciale si riferisce a comportamenti posti in essere dagli Amministratori, Dirigenti, Dipendenti di VEGA nelle aree di attività a rischio, nonché dai Collaboratori esterni e Partner, già definiti nella Parte Generale (qui di seguito tutti denominati "Destinatari").

Obiettivo della presente Parte Speciale è che tutti i Destinatari come sopra individuati, adottino regole di condotta conformi a quanto prescritto dalla stessa, al fine di impedire il verificarsi dei reati previsti nel Decreto.

4. PRESIDI DI CONTROLLO PRESCRITTI

Si evidenzia che rientrano tra le misure di prevenzione sempre applicabili:

- i principi comportamentali inseriti nel Codice Etico;
- i Principi di Controllo Generali indicati nella Parte Generale del presente Modello.

VEGA, pertanto oltre ai principi sopraccitati, prevede l'espresso obbligo, a carico di tutte le Funzioni Aziendali e dei Partner, di:

- perseguire una stretta osservanza di tutte le leggi, regolamenti e procedure che disciplinano l'attività aziendale, con particolare riferimento alle attività che comportano contatti e rapporti con la Pubblica Amministrazione ed alle attività relative allo svolgimento di una pubblica funzione o di un pubblico servizio;
- predisposizione di procedure e/o prassi atte ad impedire che un intero processo sia gestito autonomamente da un solo soggetto;
- instaurare e mantenere qualsiasi rapporto con la Pubblica Amministrazione, nell'ambito delle procure e mansioni attribuite o ricoperte in casi specifici, sulla base di criteri di massima correttezza e trasparenza;
- instaurare e mantenere qualsiasi rapporto con i terzi in tutte le attività relative allo svolgimento di una pubblica funzione o di un pubblico servizio sulla base di criteri di correttezza e trasparenza che garantiscano il buon andamento della funzione o servizio e l'imparzialità nello svolgimento degli stessi ;

- comunicare, archiviare e conservare i risultati delle attività di vigilanza della Pubblica Amministrazione;
- non porre in essere comportamenti tali da integrare le fattispecie di reato considerate agli artt. 24 e 25 del Decreto;
- non porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;
- non porre in essere qualsiasi situazione di conflitto di interessi nei confronti dei Pubblici Ufficiali, Incaricati di Pubblico servizio o della Pubblica Amministrazione in relazione a quanto previsto dalle suddette ipotesi di reato.

La presente Parte Speciale definisce, inoltre, i seguenti **Principi di Controllo Specifici** prevedendo:

1. **divieto di stipula di contratti in autonomia:** il soggetto che intrattiene rapporti o effettua negoziazioni con la Pubblica Amministrazione non cura autonomamente la stipulazione dei contratti che ha negoziato;
2. **divieto di accesso a risorse finanziarie in autonomia:** il soggetto che intrattiene rapporti o effettua negoziazioni con la Pubblica Amministrazione non accede liberamente alle risorse finanziarie e/o autorizzare disposizioni di pagamento;
3. **divieto di conferimento di contratti di consulenza o simili in autonomia:** il soggetto che intrattiene rapporti o effettua negoziazioni con la Pubblica Amministrazione non conferisce incarichi di consulenza/prestazioni professionali;
4. **divieto di conferimento di contratti di intermediazione in autonomia:** il soggetto che intrattiene rapporti o effettua negoziazioni con la Pubblica Amministrazione non conferisce incarichi di intermediazione;

5. **divieto di concessione di utilità in autonomia:** il soggetto che intrattiene rapporti e/o effettua negoziati con la Pubblica Amministrazione non concede qualsivoglia utilità;

6. **selezione ed assunzione del personale:**
 - a) divieto di assunzione di personale in autonomia: il soggetto che intrattiene rapporti o effettua negoziati con la Pubblica Amministrazione non procede ad assunzioni di personale (rapporti di lavoro);
 - b) criteri di selezione del personale: sono formalizzati criteri oggettivi di selezione dei candidati per verificare la coerenza delle candidature con il profilo richiesto nonché assicurare il rispetto della normativa vigente anche in riferimento alla definizione di clausole e condizioni contrattuali connesse all'assunzione del personale;

7. **sicurezza informatica:** esistono misure di sicurezza per il trattamento informatico dei dati, quali quelle contenute nelle leggi vigenti e negli standard internazionali di Information Security Management System;

8. **gestione di finanziamenti agevolati:** esiste segregazione di ruoli e responsabilità nelle fasi di istanza, gestione e rendicontazione in riferimento a finanziamenti agevolati, contribuzioni o altre agevolazioni;

9. **procedure di approvvigionamento beni, lavori e/o servizi:** esistono strumenti normativi relativi al processo di approvvigionamento di beni, lavori e/o servizi che prevedono:
 - trasparenza e identificazione dei ruoli: le norme aziendali sono ispirate, per ciascuna fase del processo di approvvigionamento, a criteri di trasparenza nei comportamenti e all'individuabilità dei soggetti responsabili del processo;

- modalità di approvvigionamento: esistono procedure che disciplinino la scelta della modalità di approvvigionamento da adottare (fornitore unico, utilizzo di vendor list qualificate, ecc);
 - in caso di appalto, che si tenga conto dei requisiti tecnico-professionali degli appaltatori, ivi inclusi i requisiti di carattere generale, morale e di onorabilità e che si definiscano ruoli, responsabilità e modalità di monitoraggio sul rispetto delle normative di salute, sicurezza e igiene da parte dei fornitori nonché sulle attività da questi effettuate nei confronti dei sub-appaltatori in merito al rispetto delle suddette normative;
 - modello di valutazione delle offerte: esiste un modello di valutazione delle offerte (tecniche/economiche) improntato alla trasparenza ed alla maggiore limitazione possibile di criteri di soggettività;
 - approvvigionamenti in condizioni di urgenza: sono chiaramente definite le condizioni di urgenza in relazione alle quali si può commissionare direttamente la fornitura e devono essere definiti adeguati strumenti autorizzativi e di monitoraggio (report sottoposti ad adeguato livello gerarchico);
 - Conservazione documentazione: deve esistere uno strumento normativo che indichi le modalità di archiviazione della documentazione relativa alla fornitura;
10. Deve essere adottato e attuato uno strumento normativo che preveda, laddove esponenti aziendali siano stati destinatari di richieste di rendere o produrre davanti all'Autorità Giudiziaria dichiarazioni utilizzabili in un procedimento penale relative all'esercizio delle proprie funzioni, il divieto di indurre o favorire i medesimi esponenti a non rendere/produrre le suddette dichiarazioni, ovvero a renderle mendaci



Modello di organizzazione, gestione e controllo – aggiornamento 2016
ex decreto legislativo 8 giugno 2001, n. 231

Se in via eccezionale un'attività aziendale, per un qualunque motivo, non è gestita secondo le previsioni dei presidi specifici di controllo di cui sopra, è comunque necessario il verificarsi contemporaneo delle seguenti condizioni :

- autorizzazione formale: esiste un'autorizzazione formalizzata preventiva (del Presidente o di un Dirigente incaricato) allo svolgimento dell'attività in oggetto, con evidenza e motivazione della ricorrenza del caso eccezionale, nonché modalità operative, limiti, vincoli e responsabilità;
- reportistica: predisposizione e archiviazione di verbali/report inviati al superiore gerarchico e da questi validati, dettagliati per ogni singola operazione nonché, ove applicabile, con descrizione delle modalità di gestione delle risorse finanziarie, relativi documenti giustificativi e attestazione di inerenza e congruità dell'operazione.

In ogni caso, si specifica che nell'ambito dei suddetti presidi è fatto comunque divieto di:

- effettuare elargizioni in denaro a pubblici funzionari;
- distribuire omaggi e regali al di fuori di quanto previsto dalla prassi aziendale, vale a dire, ogni forma di regalo eccedente le normali pratiche commerciali o di cortesia, o comunque rivolta ad acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale. In particolare, è vietata qualsiasi forma di regalo a funzionari pubblici, o a loro familiari, che possa influenzarne la discrezionalità o l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per l'azienda. Gli omaggi consentiti si caratterizzano sempre per la modicità del loro valore, o perché volti a promuovere l'immagine della Società. Tutti i regali offerti, salvo quelli di esiguo valore, devono essere documentati in modo idoneo, per consentire all'Organismo di Vigilanza di effettuare verifiche al riguardo;
- accordare altri vantaggi di qualsiasi natura (promesse di assunzione, ecc.) in favore di rappresentanti della Pubblica Amministrazione che possano determinare le stesse conseguenze previste al precedente punto;



*Modello di organizzazione, gestione e controllo – aggiornamento 2016
ex decreto legislativo 8 giugno 2001, n. 231*

- stipulare contratti non in forma scritta con i Fornitori e riconoscere compensi in che non trovino adeguata giustificazione in relazione al tipo di prestazione da svolgere ed alle prassi vigenti in ambito locale;
- presentare dichiarazioni non veritiere ad 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.



*Modello di organizzazione, gestione e controllo – aggiornamento 2016
ex decreto legislativo 8 giugno 2001, n. 231*

DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI

(ART.24-BIS)

1. LA TIPOLOGIA DEI REATI PREVISTI DALL'ART. 24 BIS DEL DECRETO

Per quanto concerne la presente Parte Speciale, si provvede di seguito a fornire una indicazione dei reati contemplati nell'art. 24-bis del Decreto:

Con la legge 18 marzo 2008, n. 48 l'art. 24-bis è stato inserito nel testo del Decreto, aggiungendosi alla fattispecie di frode informatica in danno dello Stato o di altro ente pubblico, già elencata tra i delitti presupposto dall'art. 24 del decreto:

- Falsità materiale e ideologica di documenti e certificazioni, uso di atto falso (Art. 491-bis c.p.)
- Accesso abusivo al sistema informatico o telematico (Art. 615-ter c.p.)
- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (Art. 615-quater c.p.)
- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (Art. 617-quater c.p.)
- Installazione d'apparecchiature per intercettare, impedire od interrompere comunicazioni informatiche o telematiche (Art. 617-quinquies c.p.)
- Danneggiamento di informazioni, dati e programmi informatici (Art. 635-bis c.p.)
- Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o di pubblica utilità (Art. 635-ter c.p.)
- Danneggiamento di sistemi informatici o telematici (Art. 635-quater c.p.)
- Danneggiamento di sistemi informatici o telematici di pubblica utilità (Art. 635-quinquies c.p.)

2. LE AREE DI ATTIVITA' A RISCHIO

In relazione a ciascuna delle tipologie di reati sopra descritte può delinearsi una specifica area a rischio.



*Modello di organizzazione, gestione e controllo – aggiornamento 2016
ex decreto legislativo 8 giugno 2001, n. 231*

Vengono qui descritte, sulla base di mere ipotesi di comportamenti delittuosi nell'ambito del processo aziendale di riferimento, le aree ritenute più specificamente a rischio:

- 1) Pianificazione generale delle misure da adottare in materia di sicurezza del sistema informatico e telematico, classificazione e trattamento di dati e informazioni;
- 2) Gestione delle modalità di accesso al sistema informatico degli utenti interni ed esterni, gestione dei profili utente e del processo di autenticazione;
- 3) Gestione delle attività di inventariazione, affidamenti ed utilizzo dei beni informatici;
- 4) Gestione e Protezione dei software, del hardware, compresa la sicurezza fisica, dei dispositivi di rete e di comunicazione e protezione delle postazioni di lavoro fisse e mobili;
- 5) Gestione delle attività di acquisizione e sviluppo di apparecchiature, dispositivi (anche di rilevazione) o programmi informatici e di servizi di installazione, manutenzione, connessione o di altra natura relativi a hardware, software e reti e relative componenti tecniche connesse con il sistema;
- 6) Monitoraggio / verifica periodica del sistema informatico in tema di sicurezza;
- 7) Gestione degli incidenti e dei problemi di sicurezza informatica.

Per ognuna delle citate aree di attività ritenute a rischio sono stati identificati i processi aziendali e i controlli per ridurre il rischio dei comportamenti illeciti.

3. DESTINATARI DELLA PARTE SPECIALE

La presente Parte Speciale si riferisce a comportamenti posti in essere dagli Amministratori, Dirigenti, Dipendenti di VEGA, nelle aree di attività a rischio, nonché dai Collaboratori esterni e Partner, già definiti nella Parte Generale (qui di seguito tutti denominati "Destinatari").



Obiettivo della presente Parte Speciale è che tutti i Destinatari come sopra individuati, adottino regole di condotta conformi a quanto prescritto dalla stessa, al fine di impedire il verificarsi dei reati previsti nel Decreto.

4. PRESIDI DI CONTROLLO PRESCRITTI

La presente Parte Speciale prevede l'espresso divieto a carico dei Destinatari di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da integrare le fattispecie di reato sopra considerate (art. 24 bis del Decreto);
- porre in essere, collaborare o dare causa alla realizzazione di comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo.

Si evidenzia che rientrano tra le misure di prevenzione sempre applicabili:

- i principi comportamentali inseriti nel Codice Etico;
- i Principi di Controllo Generali indicati nella Parte Generale del presente Modello.

La presente Parte Speciale definisce, inoltre, i seguenti **Principi di Controllo Specifici** prevedendo:

- A) **sicurezza informatica**: esistono misure di sicurezza per il trattamento informatico dei dati, quali quelle contenute nelle leggi vigenti e negli standard internazionali di Information Security Management System;
- B) **Disposizioni sulla sicurezza informatica**: le disposizioni in materia di sicurezza del sistema informatico e telematico adottate dalla Società includono:
- l'identificazione dei ruoli e delle responsabilità dei soggetti coinvolti;
 - i rapporti con gli outsourcer informatici e le modalità di aggiornamento delle stesse, anche a seguito di cambiamenti significativi;
 - le esigenze di carattere legale con riferimento alle clausole contrattuali relative alla sicurezza informatica e telematica;



- la definizione dei principi di classificazione dei dati e delle informazioni (confidenzialità, autenticità e integrità);
 - la definizione di ruoli e responsabilità nel trattamento dei dati e delle informazioni.
- C) **Organizzazione della sicurezza per gli utenti interni ed esterni:** la Società definisce ruoli e responsabilità degli utenti interni ed esterni all'azienda e i connessi obblighi nell'utilizzo del sistema informatico e delle risorse informatiche e telematiche anche con riferimento all'accesso a risorse telematiche in possesso di enti terzi la cui gestione del sistema di sicurezza ricade sulla parte terza stessa;
- D) **Sicurezza fisica:** la Società dispone l'adozione di controlli al fine di prevenire accessi non autorizzati, danni e interferenze ai locali e ai beni in essi contenuti tramite la messa in sicurezza delle aree e delle apparecchiature con particolare attenzione ai locali dedicati ai centri di elaborazione dati gestiti direttamente; la Società dispone, inoltre, l'adozione di controlli al fine di prevenire danni e interferenze alle apparecchiature gestiti direttamente che garantiscono la connettività e le comunicazioni;
- E) **Gestione delle comunicazioni e dell'operatività:** la sicurezza del sistema informatico e telematico viene garantita da parte della Società attraverso l'adozione delle misure più consone alla tipologia dell'apparato e alla catena tecnologica in esame, tra le quali:
- le misure volte a garantire e monitorare la disponibilità degli elaboratori di informazioni (valido per tutte le applicazioni sulla base delle funzionalità di sicurezza disponibili e per le basi dati e i sistemi operativi da esse sottese);
 - la protezione da software pericoloso (es. worm e virus) (valido, sottoforma di antivirus per gli ambienti microsoft e di patch management per gli altri sistemi e apparati di comunicazione come router, switch e per apparati firewall);

- il backup di informazioni di uso centralizzato e del software applicativo ritenuto critico (valido per le applicazioni e basi dati da esse sottese) nonché delle informazioni salvate nelle aree condivise centralizzate;
- la previsione di strumenti di protezione idonei a garantire la sicurezza nello scambio di informazioni critiche per il business aziendale e di carattere confidenziale anche con terzi;
- gli strumenti per effettuare:
 - la registrazione delle attività eseguite sulle applicazioni, sui sistemi e sulle reti che abbiano diretto impatto sulla sicurezza o relative agli accessi alle risorse informatiche e telematiche;
 - la registrazione delle attività effettuate dagli utenti verso l'esterno della rete aziendale (es. traffico http);
 - la protezione delle informazioni registrate (log) contro accessi non autorizzati;
- una verifica periodica/a evento dei log che registrano, per quanto rilevante ai fini della sicurezza, gli eventi, le attività degli utilizzatori e le eccezioni (valido per applicazioni e per apparati a diretto impatto sulla sicurezza perimetrale (proxy, firewall, IDS, Router));
- il controllo che i cambiamenti effettuati agli elaboratori e ai sistemi (valido per le applicazioni e per apparati a diretto impatto sulla sicurezza perimetrale (proxy, firewall, IDS, Router) non alterino i livelli di sicurezza;
- la definizione delle regole per la corretta custodia dei dispositivi di memorizzazione (ad es. pc, telefoni, chiavi USB, CD, hard disk esterni, etc.).

F) **Controllo degli accessi:** l'accesso alle informazioni, al sistema informatico, alla rete, ai sistemi operativi e alle applicazioni viene sottoposto a controllo da parte della Società attraverso l'adozione delle misure più consone alla tipologia dell'apparato e alla catena tecnologica in esame, tra le quali:

- l'autenticazione individuale e le autorizzazioni specifiche dei diversi utenti o categorie di utenti degli utenti tramite codice identificativo dell'utente e password od altro sistema di autenticazione sicura;
- procedimenti di registrazione e deregistrazione per accordare e revocare, in caso di cessazione o cambiamento del tipo di rapporto o dei compiti assegnati l'accesso a tutti i sistemi e servizi informativi, anche di terzi;
- l'accesso ai servizi di rete esclusivamente da parte degli utenti specificamente autorizzati e le restrizioni della capacità degli utenti di connettersi alla rete, (anche se tali diritti permettono di connettersi a reti e dispositivi di terze parti, la cui gestione del sistema di sicurezza ricade sulla parte terza stessa);
- la chiusura di sessioni inattive dopo un limitato periodo di tempo (valido per le postazioni di lavoro, come ad esempio screen saver).

G) **Gestione degli incidenti e dei problemi di sicurezza informatica:** il trattamento degli incidenti e dei problemi relativi alla sicurezza informatica include:

- l'adozione di canali gestionali per la comunicazione degli Incidenti e Problemi;
- la gestione dei problemi che hanno generato uno o più incidenti, fino alla loro soluzione definitiva;

H) **Sicurezza nell'acquisizione, sviluppo e manutenzione del sistema informatico:** la Società identifica i requisiti di sicurezza e di conformità tecnica (ove applicabile) in fase di acquisizione, sviluppo, fornitura e manutenzione del sistema informatico (inclusivo di componente hardware, software e delle componenti tecniche connesse).

I) **Amministratori di sistema:** la Società adempie alle prescrizioni del Garante per la protezione dei dati personali in tema di attribuzione delle funzioni di



amministratore di sistema di cui al provvedimento emesso in data 27 novembre 2008 e successive modifiche, con riferimento, in particolare, a quanto segue:

- la valutazione delle caratteristiche soggettive;
- le designazioni individuali;
- l'elenco degli amministratori di sistema;
- i servizi in outsourcing (servizi forniti da terze parti);
- la verifica delle attività;
- la registrazione degli accessi.

L) **Classificazione e controllo dei beni:** la Società assicura l'inventariazione degli asset aziendali (includere le basi dati in essi contenute) utilizzati ai fini dell'operatività del sistema informatico e telematico e adotta politiche di conformità legale (copyright), ove applicabili;



*Modello di organizzazione, gestione e controllo – aggiornamento 2016
ex decreto legislativo 8 giugno 2001, n. 231*

DELITTI DI CRIMINALITA' ORGANIZZATA

(ART. 24 TER)

1. LA TIPOLOGIA DEI REATI PREVISTI DALL'ART. 24 TER DEL DECRETO

Per quanto concerne la presente Parte Speciale, si provvede di seguito a fornire una breve descrizione dei reati in essa contemplati, indicati nell'art. 24-ter del Decreto introdotto .

L'art. 24-ter del Decreto opera un rinvio generale "aperto" a tutte le ipotesi attuali e future di reati come di seguito specificati:

- associazione per delinquere (art. 416 c.p.);
- associazioni di tipo mafioso anche straniere (art. 416-bis c.p.);
- sequestro di persona a scopo di rapina o di estorsione (art. 630 c.p.);
- reati commessi avvalendosi delle condizioni previste dall'art. 416-bis c.p. ovvero al fine di agevolare l'attività delle associazioni previste dallo stesso art. 416-bis c.p.;
- delitti previsti dall'art. 74 d.p.r. 9-10-1990, n. 309.

2. LE AREE DI ATTIVITA' A RISCHIO

In relazione a ciascuna delle tipologie di reati sopra descritte è **stata individuata la seguente area di attività a rischio:**

- 1) rapporti con singoli ed enti privati anche stranieri.

Si precisa che l'art. 24-ter fa riferimento ai delitti di criminalità organizzata, e non ai reati-fine perseguiti dalle singole associazioni, e che quindi i presidi richiesti dal modello conforme al d. lgs. n. 231/2001 sono posti a prevenzione dell'autonomo delitto di associazione vietata, e non dei singoli delitti-fine, costituenti una pletera di fattispecie indefinita e quindi oggettivamente non mappabile.

3. DESTINATARI DELLA PARTE SPECIALE

Destinatari della presente Parte Speciale sono gli Amministratori, i dirigenti preposti alla redazione dei documenti contabili societari, rappresentanti e procuratori di VEGA, i sindaci, nonché il personale (dipendente e non) soggetto a vigilanza e controllo da parte dei soggetti apicali nelle aree di attività a rischio, qui di seguito tutti denominati "Destinatari".

Obiettivo della presente Parte Speciale è che tutti i Destinatari come sopra individuati siano precisamente consapevoli della valenza dei comportamenti censurati e che quindi adottino regole di condotta conformi a quanto prescritto dalla stessa, al fine di impedire il verificarsi dei reati previsti nel Decreto.

4. PRESIDI DI CONTROLLO PRESCRITTI

La presente Parte Speciale prevede l'espresso divieto a carico dei Destinatari di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da integrare le fattispecie di reato sopra considerate (art. 24-ter del Decreto);
- porre in essere, collaborare o dare causa alla realizzazione di comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo.

Si evidenzia che rientrano tra le misure di prevenzione sempre applicabili:

- i principi comportamentali inseriti nel Codice Etico;
- i Principi di Controllo Generali indicati nella Parte Generale del presente Modello.

VEGA, pertanto oltre ai principi sopraccitati, prevede l'espresso obbligo, a carico di tutte le Funzioni Aziendali e dei Partner:

- divieto di promozione, finanziamento o sponsorizzazione di associazioni (anche ONLUS e ONG) attraverso l'attribuzione di appalti/contratti ad appartenenti ad organizzazioni che compiono attività violente con finalità eversive o di terrorismo anche verso uno Stato estero o un organismo internazionale;

- divieto di concessione di ospitalità o sostegno abitativo ad appartenenti ad organizzazioni che compiono attività violente con finalità eversive o di terrorismo anche verso uno Stato estero o un organismo internazionale;
- divieto di concessione di vitto o viveri ad appartenenti ad organizzazioni che compiono attività violente con finalità eversive o di terrorismo anche verso uno Stato estero o un organismo internazionale;
- divieto di concessione di mezzi di trasporto personali o dell'ente ad appartenenti ad organizzazioni che compiono attività violente con finalità eversive o di terrorismo anche verso uno Stato estero o un organismo internazionale

A) divieto di conferimento di contratti di intermediazione in autonomia: il soggetto che intrattiene rapporti o effettua negoziazioni con la Pubblica Amministrazione non conferisce incarichi di intermediazione;

B) selezione ed assunzione del personale:

- divieto di assunzione di personale in autonomia: il soggetto che intrattiene rapporti o effettua negoziazioni con la Pubblica Amministrazione non procede ad assunzioni di personale (rapporti di lavoro);
- criteri di selezione del personale: sono formalizzati criteri oggettivi di selezione dei candidati per verificare la coerenza delle candidature con il profilo richiesto nonché assicurare il rispetto della normativa vigente anche in riferimento alla definizione di clausole e condizioni contrattuali connesse all'assunzione del personale;

C) Deve essere adottato e attuato uno strumento normativo che annoveri la verifica preventiva dell'inesistenza di **relazioni privilegiate** tra gli esponenti della Società e gli esponenti della Pubblica Amministrazione locale e/o fornitori, clienti o terzi contraenti della Società. In caso sia verificata l'esistenza di relazioni

privilegiate, la nomina dovrà essere sottoposta all'approvazione dell'Amministratore Delegato o di un dirigente da questi incaricato;

D) Deve essere adottato e attuato uno strumento normativo che preveda, laddove esponenti aziendali siano stati destinatari di richieste di rendere o produrre davanti all'Autorità Giudiziaria dichiarazioni utilizzabili in un procedimento penale relative all'esercizio delle proprie funzioni, **il divieto di indurre o favorire i medesimi esponenti a non rendere/produire le suddette dichiarazioni, ovvero a renderle mendaci;**

E) Deve esistere il **divieto** di:

- intrattenere rapporti, negoziare e/o stipulare e/o porre in esecuzione contratti o atti con persone indicate nelle **Liste di Riferimento** o facenti parte di organizzazioni presenti nelle stesse;
- concessione di utilità a persone indicate nelle **Liste di Riferimento** o facenti parte di organizzazioni presenti nelle stesse;
- assumere persone indicate nelle **Liste di Riferimento** o facenti parte di organizzazioni presenti nelle stesse.

F) Deve essere adottato e attuato uno **strumento normativo** che annoveri:

- la verifica preventiva dei presupposti di carattere strategico, economico e finanziario nonché dell'attuabilità della **proposta di investimento** da parte di un organo/unità;
- la verifica preventiva dei **requisiti di onorabilità e professionalità dei partner** commerciali/finanziari;

G) Liberalità: deve essere adottato uno strumento normativo che, nel caso si intendesse procedere con la concessione di qualsiasi liberalità, preveda:

- l'elaborazione ed approvazione di un budget;
- una verifica preliminare sul potenziale beneficiario;



*Modello di organizzazione, gestione e controllo – aggiornamento 2016
ex decreto legislativo 8 giugno 2001, n. 231*

- adeguati controlli sui flussi finanziari in uscita;
- il monitoraggio e la consuntivazione dell'iniziativa.

H) **Sponsorizzazioni:** deve essere adottato uno strumento normativo che, nel caso si intendesse procedere con la concessione di qualsiasi sponsorizzazione, preveda:

- l'analisi dei potenziali benefit;
- una verifica preliminare sul potenziale beneficiario;
- adeguati controlli sui flussi finanziari in uscita;
- il monitoraggio e la consuntivazione dell'iniziativa.



*Modello di organizzazione, gestione e controllo – aggiornamento 2016
ex decreto legislativo 8 giugno 2001, n. 231*

REATI SOCIETARI

(ART. 25 TER)

1. LA TIPOLOGIA DEI REATI SOCIETARI (ART. 25 TER DEL DECRETO)

Per quanto concerne la presente Parte Speciale, si provvede di seguito ad elencare reati in essa contemplati, indicati nell'art. 25 ter del Decreto, e che si possono raggruppare in 5 tipologie.

FALSITA' IN COMUNICAZIONI, PROSPETTI E RELAZIONI

- 1) *False comunicazioni sociali (artt. 2621 e 2622 c.c.)*
- 2) *Falsità nelle relazioni o nelle comunicazioni delle società di revisione (art. 2624 c.c.)*

TUTELA PENALE DEL CAPITALE SOCIALE

- 1) *Indebita restituzione dei conferimenti (art. 2626 c.c.)*
- 2) *Illegale ripartizione degli utili o delle riserve (art. 2627 c.c.)*
- 3) *Illecite operazioni sulle azioni o quote sociali proprie o della società controllante (art. 2628 c.c.)*
- 4) *Operazioni in pregiudizio dei creditori (art. 2629 c.c.)*
- 5) *Formazione fittizia del capitale (art. 2632 c.c.)*
- 6) *Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.)*

TUTELA PENALE DEL REGOLARE FUNZIONAMENTO DELLA SOCIETÀ

- 1) *Impedito controllo (art. 2625 c.c.)*
- 2) *Illecita influenza sull'assemblea (art. 2636 c.c.)*

TUTELA PENALE CONTRO LE FRODI

- 1) *Aggiotaggio (art. 2637 c.c.)*

TUTELA PENALE DELLE FUNZIONI DI VIGILANZA

- 1) *Ostacolo all'esercizio delle funzioni delle autorità Pubbliche di vigilanza (art. 2638 c.c.)*

2. LE AREE DI ATTIVITA' A RISCHIO

In relazione a ciascuna delle tipologie di reati sopra descritte possono delinearsi le seguenti aree a rischio sulla base di mere ipotesi di comportamenti delittuosi nell'ambito del processo aziendale di riferimento:

1. Predisposizione dei bilanci, delle relazioni o delle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, nonché nel caso di rilascio di attestazioni richieste dalla legge;
2. Gestione dei rapporti con soci, Società di revisione e Collegio Sindacale;
3. Gestione delle Operazioni sul Capitale Sociale e destinazione dell'utile;
4. Gestione adempimenti societari.

Per ognuna delle citate aree di attività ritenute a rischio sono stati identificati i processi aziendali e i controlli per ridurre il rischio dei comportamenti illeciti.

Per ognuna delle citate aree di attività ritenute a rischio sono stati identificati i processi aziendali e i controlli per ridurre il rischio dei comportamenti illeciti.

3. DESTINATARI DELLA PARTE SPECIALE

Destinatari della presente Parte Speciale sono gli amministratori, i dirigenti preposti alla redazione dei documenti contabili societari, rappresentanti e procuratori di VEGA, i sindaci, nonché il personale (dipendente e non) soggetto a vigilanza e controllo da parte dei soggetti apicali nelle aree di attività a rischio, qui di seguito tutti denominati "Destinatari".

Per quanto concerne gli amministratori, direttori generali ed i liquidatori, la legge equipara a coloro che sono formalmente investiti di tali qualifiche anche i soggetti che svolgono tali funzioni "di fatto". Ai sensi dell'art. 2639 c.c., infatti, dei reati societari previsti dal codice civile, risponde sia chi è tenuto a svolgere la stessa funzione, diversamente qualificata, sia chi esercita in modo continuativo e significativo i poteri tipici inerenti alla qualifica o alla funzione.

Obiettivo della presente Parte Speciale è che tutti i Destinatari come sopra individuati siano precisamente consapevoli della valenza dei comportamenti censurati e che quindi adottino regole di condotta conformi a quanto prescritto dalla stessa, al fine di impedire il verificarsi dei reati previsti nel Decreto.

4. PRESIDI DI CONTROLLO PRESCRITTI

La presente Parte Speciale prevede l'espresso divieto a carico dei Destinatari di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da integrare le fattispecie di reato sopra considerate (art. 25 ter del Decreto);
- porre in essere, collaborare o dare causa alla realizzazione di comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo.

Si evidenzia che rientrano tra le misure di prevenzione sempre applicabili:

- i principi comportamentali inseriti nel Codice Etico;
- i Principi di Controllo Generali indicati nella Parte Generale del presente Modello.



Modello di organizzazione, gestione e controllo – aggiornamento 2016
ex decreto legislativo 8 giugno 2001, n. 231

VEGA, pertanto oltre ai principi sopraccitati, prevede l'espresso obbligo, a carico di tutte le Funzioni Aziendali e dei Partner, di:

- 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 ai soci ed ai terzi una informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della società;
- di osservare rigorosamente tutte le norme poste dalla legge a tutela dell'integrità ed effettività del capitale sociale e di agire sempre nel rispetto delle procedure interne aziendali che su tali norme si fondano, al fine di non ledere le garanzie dei creditori e dei terzi in genere;
- di assicurare il regolare funzionamento della società e degli organi sociali, garantendo ed agevolando ogni forma di controllo interno sulla gestione sociale previsto dalla legge nonché, la libera e corretta formazione della volontà assembleare;
- di effettuare con tempestività, correttezza e buona fede tutte le comunicazioni previste dalla legge e dai regolamenti nei confronti delle Autorità di Vigilanza, non frapponendo alcun ostacolo all'esercizio delle funzioni di vigilanza da queste esercitate.

La presente Parte Speciale definisce, inoltre, i seguenti **Principi di Controllo Specifici**:

sicurezza informatica: esistono misure di sicurezza per il trattamento informatico dei dati, quali quelle contenute nelle leggi vigenti e negli standard internazionali di Information Security Management System;

Procedure contabili: devono esistere ed essere diffusi al personale coinvolto in attività di predisposizione dei documenti contabili, strumenti normativi di gruppo che definiscano con chiarezza i principi contabili da adottare per la definizione delle



*Modello di organizzazione, gestione e controllo – aggiornamento 2016
ex decreto legislativo 8 giugno 2001, n. 231*

informazioni e dati sulla situazione economica, patrimoniale e finanziaria della Società e delle modalità operative per la loro contabilizzazione.

Istruzioni di chiusura contabile: devono esistere istruzioni rivolte alle Unità/Direzioni/Società, con cui si stabilisca quali dati e notizie debbano essere forniti all'Amministrazione in relazione alle chiusure annuali (per i documenti contabili societari), con quali modalità e la relativa tempistica.

Contratto di servizio: esistenza di un modello di servizio previsto contrattualmente tra la Società e la società di servizi incaricata, che preveda ruoli, responsabilità nel caso in cui la predisposizione dei documenti contabili societari sia eseguita in outsourcing.

Lettere di attestazione: il Presidente dell'Ente e la massima carica amministrativa devono rilasciare le lettere che attestano la corrispondenza dei dati e delle informazioni fornite ai fini della redazione dei documenti contabili societari alle risultanze documentali, ai libri e dalle scritture contabili al soggetto incaricato del controllo ex art. 2409 bis codice civile.

Conservazione del fascicolo di bilancio e degli altri documenti contabili societari: esistono regole che identificano ruoli e responsabilità, relativamente alla tenuta, conservazione e aggiornamento del fascicolo di bilancio e degli altri documenti contabili societari (ivi incluse le relative attestazioni) dalla loro formazione ed eventuale approvazione del Consiglio di Amministrazione al deposito e pubblicazione (anche informatica) dello stesso e alla relativa archiviazione.

Gestione del verbale d'assemblea: esiste uno strumento normativo che identifica ruoli e responsabilità, relativamente alla trascrizione ed archiviazione del verbale d'assemblea.

deve essere adottato e attuato uno strumento normativo che disponga la richiesta preventiva a tutti i partecipanti alla riunione di un Consiglio di Amministrazione di dichiarare, all'apertura della riunione, la **sussistenza di interessi la cui comunicazione sia richiesta nelle forme prescritte dall'art. 2391 comma 1 c.c.**

In ogni caso, si specifica che nell'ambito dei suddetti presidi è fatto comunque divieto di:

- rappresentare o trasmettere per l'elaborazione e la rappresentazione in bilanci, relazioni e prospetti o altre comunicazioni sociali, dati falsi, lacunosi o, comunque, non rispondenti alla realtà, sulla situazione economica, patrimoniale e finanziaria della società;
- omettere la comunicazione di dati ed informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria della Società;
- restituire conferimenti ai soci o liberare gli stessi dall'obbligo di eseguirli, al di fuori del caso di legittima riduzione del capitale sociale, in qualsiasi forma non specificamente ricompresa fra quelle qui di seguito descritte;
- ripartire utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva;
- acquistare o sottoscrivere azioni della Società fuori dai casi previsti dalla legge;
- effettuare riduzioni del capitale sociale, fusioni o scissioni, in violazione delle disposizioni di legge a tutela dei creditori;
- procedere a formazione o aumento fittizi del capitale sociale, attribuendo azioni o quote per un valore inferiore al loro valore nominale in sede di costituzione di società o di aumento del capitale sociale;
- distrarre i beni sociali, in sede di liquidazione della società, dalla loro destinazione ai creditori, ripartendoli fra i soci prima del pagamento dei creditori o dell'accantonamento delle somme necessarie a soddisfarli;
- porre in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, o che comunque

- costituiscano ostacolo allo svolgimento all'attività di controllo o di revisione della gestione sociale da parte del Collegio Sindacale ;
- determinare o influenzare l'assunzione delle deliberazioni dell'assemblea, ponendo in essere atti simulati o fraudolenti finalizzati ad alterare il regolare procedimento di formazione della volontà assembleare;
 - omettere di effettuare, con la dovuta qualità e tempestività, tutte le segnalazioni periodiche previste dalle leggi e dalla normativa di settore nei confronti delle alle Autorità di Vigilanza cui è soggetta l'attività aziendale, nonché la trasmissione dei dati e documenti previsti dalla normativa e/o specificamente richiesti dalle predette Autorità;
 - esporre nelle predette comunicazioni e trasmissioni fatti non rispondenti al vero, ovvero occultare fatti rilevanti, in relazione alle condizioni economiche, patrimoniali o finanziarie della società;
 - porre in essere qualsiasi comportamento che sia di ostacolo all'esercizio delle funzioni di vigilanza anche in sede di ispezione da parte delle Autorità Pubbliche di Vigilanza (espressa opposizione, rifiuti pretestuosi, o anche comportamenti ostruzionistici o di mancata collaborazione, quali ritardi nelle comunicazioni o nella messa a disposizione di documenti).

Gli strumenti di controllo sono attuati da:

- società di revisione
- collegio sindacale
- ODV

attraverso incontri periodici organizzati a richiesta da parte dei suddetti organi, in cui sono segnalate, evidenziate eventuali criticità ed in cui sono identificate le modalità di risoluzione.



Modello di organizzazione, gestione e controllo – aggiornamento 2016
ex decreto legislativo 8 giugno 2001, n. 231

**REATI DI OMICIDIO COLPOSO E LESIONI COLPOSE GRAVI O
GRAVISSIME, COMMESSI CON VIOLAZIONI DELLE NORMA
ANTINFORTUNISTICHE E SULLA TUTELA DELL'IGIENE E
DELLA SALUTE SUL LAVORO**
(ART. 25 SEPTIES)

1. LA TIPOLOGIA DEI REATI PREVISTI DALL'ART. 25 SEPTIES DEL DECRETO

Per quanto concerne la presente Parte Speciale, si provvede di seguito a fornire una breve elencazione dei reati contemplati nell'art. 25 septies del Decreto introdotti dall'art. 9 della Legge n. 123 del 3 agosto 2007 così come modificato dal D.lgs 9 aprile 2008 n. 81 e dal d. lgs. 3 agosto 2009, n. 106:

- omicidio colposo (art. 589 c.p.);
- lesioni personali colpose gravi o gravissime (art. 590 c.p.).

entrambi commessi con violazione delle norme antinfortunistiche sulla tutela dell'igiene e della salute sul lavoro.

Le fattispecie criminose richiamate dall'art. 25-septies sono le seguenti:

- a) *Omicidio colposo (art. 589 c.p.)*
- b) *Lesioni personali colpose (art. 590 c.p.).*

2. LE AREE DI ATTIVITÀ A RISCHIO

In relazione a ciascuna delle tipologie di reati sopra descritte può delinearsi una specifica area a rischio.

Vengono qui descritte, sulla base di mere ipotesi di comportamenti delittuosi nell'ambito del processo aziendale di riferimento, le aree ritenute più specificamente a rischio:

- 1) Pianificazione e organizzazione dei ruoli e delle attività connesse alla tutela della salute, sicurezza e igiene sul lavoro;
- 2) Sistema di deleghe di funzione in tema di salute, sicurezza e igiene sul lavoro;
- 3) Individuazione, valutazione e gestione dei rischi in tema di salute, sicurezza e igiene sul lavoro;
- 4) Attività di informazione e formazione in tema di salute, sicurezza e igiene sul lavoro;



*Modello di organizzazione, gestione e controllo – aggiornamento 2016
ex decreto legislativo 8 giugno 2001, n. 231*

- 5) Rapporti con i fornitori con riferimento alle attività connesse alla salute, sicurezza e igiene sul lavoro;
- 6) Gestione degli asset aziendali con riferimento alle attività connesse alla salute, sicurezza e igiene sul lavoro;
- 7) Controllo e Azioni Correttive con riferimento alle attività connesse alla salute, sicurezza e igiene sul lavoro;
- 8) Riesame della Direzione con riferimento alle attività connesse alla salute, sicurezza e igiene sul lavoro.

Per ognuna delle citate aree di attività ritenute a rischio sono stati identificati i processi aziendali e i controlli per ridurre il rischio dei comportamenti illeciti.

3. DESTINATARI DELLA PARTE SPECIALE

Destinatari della presente Parte Speciale sono tutti i Dipendenti e collaboratori di VEGA qui di seguito tutti denominati "Destinatari".

Obiettivo della Parte Speciale è che tutti i Destinatari come sopra individuati siano precisamente consapevoli della valenza dei comportamenti censurati e che quindi adottino regole di condotta conformi a quanto prescritto dalla stessa, al fine di impedire il verificarsi dei reati previsti nel Decreto.

4. PRESIDI DI CONTROLLO PRESCRITTI

La presente Parte Speciale prevede l'espresso divieto a carico dei Destinatari di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da integrare le fattispecie di reato sopra considerate (art. 25 septies del Decreto);
- porre in essere, collaborare o dare causa alla realizzazione di comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo.



Si evidenzia che rientrano tra le misure di prevenzione sempre applicabili:

- i principi comportamentali inseriti nel Codice Etico;
- i Principi di Controllo Generali indicati nella Parte Generale del presente Modello.

La presente Parte Speciale definisce, inoltre, i seguenti **Principi di Controllo Specifici** prevedendo:

A) **procedure di approvvigionamento beni, lavori e/o servizi**: esistono strumenti normativi relativi al processo di approvvigionamento di beni, lavori e/o servizi che prevedono:

- trasparenza e identificazione dei ruoli: le norme aziendali sono ispirate, per ciascuna fase del processo di approvvigionamento, a criteri di trasparenza nei comportamenti e all'individuabilità dei soggetti responsabili del processo;
- modalità di approvvigionamento: esistono procedure che disciplinino la scelta della modalità di approvvigionamento da adottare (fornitore unico, utilizzo di vendor list qualificate, ecc);
- in caso di appalto, che si tenga conto dei requisiti tecnico-professionali degli appaltatori, ivi inclusi i requisiti di carattere generale e morale e che si definiscano ruoli, responsabilità e modalità di monitoraggio sul rispetto delle normative di salute, sicurezza e igiene da parte dei fornitori nonché sulle attività da questi effettuate nei confronti dei sub-appaltatori in merito al rispetto delle suddette normative;
- modello di valutazione delle offerte: esiste un modello di valutazione delle offerte (tecniche/economiche) improntato alla trasparenza ed alla maggiore limitazione possibile di criteri di soggettività;
- approvvigionamenti in condizioni di urgenza: sono chiaramente definite le condizioni di urgenza in relazione alle quali si può commissionare direttamente la fornitura e devono essere definiti adeguati strumenti

autorizzativi e di monitoraggio (report sottoposti ad adeguato livello gerarchico);

- Conservazione documentazione: deve esistere uno strumento normativo che indichi le modalità di archiviazione della documentazione relativa alla fornitura;

B) **Politica e Obiettivi**: esiste un documento formalizzato di Politica che definisca gli indirizzi e gli obiettivi generali in tema di ambiente, salute, sicurezza e igiene sul lavoro che l'azienda stabilisce di raggiungere e che:

- è formalmente approvato dalla direzione aziendale;
- contiene l'impegno ad essere conforme con le vigenti leggi in materia di salute, sicurezza e igiene applicabili e con gli altri requisiti sottoscritti;
- è adeguatamente diffuso ai dipendenti ed alle parti interessate;
- è periodicamente riesaminato per assicurare che gli obiettivi in esso indicati siano appropriati e adeguati rispetto ai rischi presenti nell'organizzazione (ad es. riesame sulla base delle Linee Guida per l'attuazione del sistema di gestione della sicurezza, ambiente, dei nuovi regolamenti e delle leggi, etc.).

C) **Adozione del SGPL** (Sistema di Gestione della Prevenzione nei luoghi di Lavoro), che ai sensi dell'art. 30 d.lgs. n. 81/2008 deve assicurare da parte delle persone fisiche operanti nell'organizzazione delle regole precauzionali fissate dal legislatore o da fonti sociali per prevenire infortuni o malattie professionali;

D) **Norme e documentazione del sistema di gestione**: deve essere adottato e attuato uno strumento normativo e/o organizzativo che:

- disciplini ruoli e responsabilità nella gestione della documentazione relativa al sistema di gestione della salute, della sicurezza, dell'ambiente e dell'incolumità pubblica (es. Manuale, Procedure, Istruzioni di lavoro) in coerenza con la Politica e le linee guida aziendali;

- definisca le modalità di gestione, archiviazione e conservazione della documentazione prodotta (es: modalità di archiviazione/protocollazione a garanzia di un adeguato livello di tracciabilità /verificabilità);
- disciplina ruoli e responsabilità dell'aggiornamento delle informazioni riguardo alla legislazione rilevante e alle altre prescrizioni applicabili in tema di salute, sicurezza e igiene sul lavoro;
- definisce criteri e modalità da adottarsi per la comunicazione degli aggiornamenti alle aree aziendali interessate

E) **Organizzazione e Responsabilità** - deve essere adottato e attuato uno strumento normativo e/o organizzativo che con riferimento alle figure del Datore di Lavoro, RSPP, SPP, Medico Competente, Incaricati alle emergenze e ove esistenti, Sorvegliante, Direttore Responsabile, Coordinatore in materia di salute, sicurezza per la progettazione dell'opera e Coordinatore in materia di sicurezza e di salute durante la realizzazione dell'opera (appalti e nei cantieri temporanei o mobili), così come previsto ai sensi della normativa vigente:

- preveda una formale designazione;
- definisca, in considerazione dell'ambito di attività, i requisiti specifici che, coerentemente alle disposizioni di legge in materia, devono caratterizzare tale figura (es. pregressa esperienza, partecipazione a particolari tipologie di corsi di formazione, titoli specifici, specifiche competenze, etc.);
- preveda la tracciabilità delle verifiche svolte in ordine al possesso dei requisiti previsti dalla normativa in materia;
- preveda la tracciabilità della formale accettazione dell'incarico.

F) **Sistema di deleghe di funzioni:** esiste un sistema di deleghe di funzioni conforme agli artt. 16 e 17 d. lgs. n. 81/2008 e tale da garantire, in capo al soggetto delegato, la sussistenza:

- di poteri decisionali coerenti con le deleghe;
- di un budget, laddove necessario in considerazione del ruolo ricoperto, per l'efficace adempimento delle funzioni delegate;

- di un obbligo di rendicontazione formalizzata sui poteri delegati, con modalità prestabilite atte a garantire un'attività di vigilanza senza interferenze.

G) **Valutazione dei rischi – Ruoli e responsabilità:** è adottato e attuato uno strumento normativo e/o organizzativo che identifica ruoli, responsabilità e modalità per lo svolgimento, approvazione e aggiornamento della valutazione dei rischi aziendali. In particolare tale norma:

- identifica ruoli, responsabilità, requisiti di competenza e necessità di addestramento del personale responsabile per condurre l'identificazione dei pericoli, l'identificazione e il controllo del rischio;
- identifica le responsabilità per la verifica, l'approvazione e l'aggiornamento dei contenuti dei documenti di valutazione dei rischi;
- identifica modalità e criteri per la revisione in tempi o periodi determinati dei processi di identificazione dei pericoli e valutazione del rischio;
- prevede, laddove necessario, la tracciabilità dell'avvenuto coinvolgimento del Medico Competente, dei Rappresentanti dei Lavoratori per la Sicurezza e l'Ambiente e delle altre figure previste dalle disposizioni normative vigenti nel processo di identificazione dei pericoli e valutazione dei rischi;
- prevede, laddove necessario, la valutazione delle diverse tipologie di sorgenti di rischio: pericoli ordinari o generici, ergonomici, specifici, di processo e organizzativi e una individuazione di aree omogenee in termini di pericolo all'interno dell'azienda;
- prevede, laddove necessario, l'individuazione delle mansioni rappresentative dei lavoratori;
- prevede, laddove necessario, il censimento e la caratterizzazione degli agenti chimici e delle attrezzature e macchine presenti;
- prevede, laddove necessario, esplicita definizione dei criteri di valutazione adottati per le diverse categorie di rischio nel rispetto della normativa e prescrizioni vigenti.

H) **Documento di valutazione dei rischi:** esiste un documento di valutazione dei rischi e la conseguente documentazione redatta secondo le disposizioni vigenti e che contengono almeno:

- il procedimento di valutazione, con la specifica individuazione dei criteri adottati;
- l'individuazione e formalizzazione delle misure di prevenzione e protezione, e dei dispositivi di protezione individuale, conseguenti alla valutazione;
- il programma delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza.

I) **Gestione delle emergenze:** è adottato e attuato uno strumento normativo e/o organizzativo per la gestione delle emergenze, atto a mitigarne gli effetti interni, nel rispetto della salute della popolazione e dell'ambiente esterno. In particolare tale norma:

- definisce ruoli, responsabilità e misure per il controllo di situazioni di rischio in caso di emergenza, atte a controllare e circoscrivere gli eventi in modo da minimizzarne gli effetti;
- definisce le modalità di abbandono del posto di lavoro o zona pericolosa in cui persiste un pericolo grave e immediato;
- definisce le modalità di intervento dei lavoratori incaricati dell'attuazione delle misure di prevenzione incendi, di evacuazione dei lavoratori in caso di pericolo grave ed immediato e di pronto soccorso;
- individua i provvedimenti atti a evitare rischi per la salute della popolazione o deterioramento dell'ambiente esterno;
- definisce le modalità e la tempistica/frequenza di svolgimento delle prove di emergenza;
- definisce l'aggiornamento delle misure di prevenzione a seguito dei progressi tecnologici e delle nuove conoscenze in merito alle misure da adottare in caso di emergenze.

- L) **Consultazione e comunicazione:** è adottato e attuato uno strumento normativo e/o organizzativo che prevede riunioni periodiche di tutte le figure competenti per la verifica della situazione nella gestione delle tematiche riguardanti ambiente, salute, sicurezza e igiene e di una adeguata diffusione delle risultanze delle riunioni all'interno dell'organizzazione.
- M) **Diffusione delle informazioni, formazione, sensibilizzazione e competenze:** è adottato e attuato uno strumento normativo e/o organizzativo che disciplini la diffusione delle informazioni previste dalla normativa vigente relative all'ambiente, salute, sicurezza e igiene. In particolare tale norma definisce:
- ruoli, responsabilità e modalità di informazione/formazione periodica delle funzioni competenti verso i lavoratori, in relazione alle tematiche ambiente, salute, sicurezza e igiene applicabili alle loro attività;
 - l'informativa del Medico Competente, laddove necessario, relativamente ai processi e rischi connessi all'attività produttiva;
 - i criteri di erogazione della formazione di ciascun lavoratore (es. all'assunzione, trasferimento o cambiamento di mansioni, introduzione di nuove attrezzature, tecnologie, sostanze pericolose);
 - l'ambito, i contenuti e le modalità della formazione in dipendenza del ruolo assunto all'interno della struttura organizzativa;
- N) **Rapporti con fornitori e contrattisti – clausole contrattuali, informazione e coordinamento:** deve essere adottato e attuato uno strumento normativo e/o organizzativo che definisca:
- ruoli, responsabilità e modalità di inserimento delle clausole contrattuali standard riguardanti il rispetto delle normative di salute, sicurezza e igiene applicabili, nonché i costi della sicurezza nei contratti di somministrazione dei lavoratori, di appalto e di subappalto;

- ruoli, responsabilità, modalità e contenuti dell'informazione da fornire alle imprese esterne sui rischi specifici esistenti nell'ambiente in cui le imprese stesse sono destinate a operare e sulle misure da adottare in relazione alla propria attività che un'impresa appaltatrice aggiudicataria deve conoscere, impegnarsi a rispettare e a far rispettare ai propri dipendenti;
 - ruoli, responsabilità e modalità di elaborazione del documento di valutazione dei rischi che indichi le misure da adottare per eliminare i rischi dovuti alle interferenze tra i lavoratori nel caso di diverse imprese coinvolte nell'esecuzione di un' opera.
- O) **Gestione degli asset:** è adottato e attuato uno strumento normativo e/o organizzativo che disciplina le attività di manutenzione/ispezione degli asset aziendali (es. attrezzature e impianti meccanici, elettrici ed elettromeccanici) affinché ne sia sempre garantita l'integrità e l'adeguatezza in termini di ambiente, salute e sicurezza dei lavoratori. In particolare tale norma:
- definisce ruoli, responsabilità e modalità di gestione degli asset;
 - prevede periodiche verifiche di adeguatezza e integrità degli asset e di conformità ai requisiti normativi applicabili;
 - prevede la pianificazione, effettuazione e verifica delle attività di ispezione e manutenzione tramite personale qualificato e idoneo.
- I presidi sotto elencati non sono obbligatori ma opportuni ai fini di un corretto SGPL:**
- P) **Misura e monitoraggio delle prestazioni, infortuni e incidenti e altri dati (diversi da infortuni e incidenti):** deve essere adottato e attuato uno strumento normativo e/o organizzativo che disciplini:
- ruoli, responsabilità e modalità di rilevazione, registrazione e investigazione interna degli infortuni;
 - ruoli, responsabilità e modalità di tracciabilità e investigazione degli incidenti occorsi e dei "mancati incidenti" e

- modalità di comunicazione da parte dei responsabili operativi al datore di lavoro e al responsabile del servizio di prevenzione e protezione sugli infortuni/incidenti occorsi;
 - ruoli, responsabilità e modalità di monitoraggio degli infortuni occorsi (tenendo conto di eventuali controversie/contenziosi pendenti relativi agli infortuni occorsi sui luoghi di lavoro) al fine di identificare le aree a maggior rischio infortuni.
 - ruoli, responsabilità e modalità di registrazione e monitoraggio (anche attraverso l'uso di indicatori) per:
 - i dati riguardanti la sorveglianza sanitaria;
 - i dati riguardanti la sicurezza degli impianti (apparecchi di sollevamento e ascensori,
 - impianti elettrici, attrezzature a pressione, serbatoi interrati, apparecchiature laser; macchine);
 - i dati riguardanti le sostanze e i preparati pericolosi utilizzati in azienda (schede di sicurezza);
 - altri dati diversi da infortuni e incidenti (tenendo conto di eventuali controversie/contenziosi insorti)
 - al fine di identificare le aree a maggior rischio.
- Q) **Audit HSE:** è adottato e attuato uno strumento normativo e/o organizzativo che disciplina ruoli, responsabilità e modalità operative riguardo le attività di audit e verifica periodica dell'efficienza ed efficacia del sistema di gestione della sicurezza. In particolare tale norma definisce:
- la tempistica per la programmazione delle attività (piano di audit formalizzato);
 - le competenze necessarie per il personale coinvolto nelle attività di audit nel rispetto del principio dell'indipendenza dell'auditor rispetto all' attività oggetto di audit;
 - le modalità di registrazione degli audit;

- le modalità di individuazione e applicazione di azioni correttive nel caso siano rilevati scostamenti rispetto a quanto prescritto dal sistema di gestione della salute, sicurezza e igiene in azienda o dalle norme e prescrizioni applicabili;
 - le modalità di verifica dell'attuazione e dell'efficacia delle suddette azioni correttive;
 - le modalità di comunicazione dei risultati dell'audit alla Direzione aziendale.
- R) **Reporting:** è adottato e attuato uno strumento normativo e/o organizzativo che disciplina ruoli, responsabilità e modalità operative delle attività di reporting verso la Direzione. Tale report deve garantire la tracciabilità e la disponibilità dei dati relativi alle attività inerenti al sistema di gestione della sicurezza e in particolare l'invio periodico delle informazioni inerenti a:
- scostamenti tra i risultati ottenuti e gli obiettivi programmati;
 - risultati degli audit;
 - risultati del monitoraggio della performance del sistema di gestione della salute, della sicurezza, dell'ambiente e dell'incolumità pubblica (infortuni, altri dati);
 - spese sostenute e risultati di miglioramento raggiunti in relazione alle suddette spese.
- S) **Conduzione del processo di riesame:** è adottato e attuato uno strumento normativo e/o organizzativo che definisce ruoli, responsabilità e modalità di conduzione del processo di riesame da parte della Direzione aziendale in relazione all'efficacia e all'efficienza del sistema di gestione della salute, della sicurezza, dell'ambiente e dell'incolumità pubblica in azienda. Tale norma prevede lo svolgimento delle seguenti attività:
- analisi delle risultanze del reporting ottenuto;
 - analisi dello stato di avanzamento di eventuali azioni di miglioramento definite nel precedente riesame;



*Modello di organizzazione, gestione e controllo – aggiornamento 2016
ex decreto legislativo 8 giugno 2001, n. 231*

- individuazione degli obiettivi di miglioramento per il periodo successivo e la necessità di eventuali modifiche ad elementi del sistema di gestione della salute, sicurezza e igiene in azienda;
- tracciabilità delle attività effettuate.



Modello di organizzazione, gestione e controllo – aggiornamento 2016
ex decreto legislativo 8 giugno 2001, n. 231

**RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O
UTILITÀ DI PROVENIENZA ILLECITA**

(ART. 25 OCTIES)

1. LA TIPOLOGIA DEI REATI PREVISTI DALL'ART. 25 OCTIES DEL DECRETO

Con il D. Lgs. n. 231 del 21 novembre 2007 - in vigore dal 29 dicembre 2007 - il legislatore ha dato attuazione alla direttiva 2005/60/CE del Parlamento e del Consiglio, del 26 ottobre 2005, concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo (c.d. III direttiva antiriciclaggio), e alla direttiva 2006/70/CE della Commissione che ne reca misure di esecuzione.

Per quanto concerne la presente Parte Speciale, si provvede di seguito a fornire una breve descrizione dei reati contemplati nell'art. 25 octies del Decreto introdotti dall'art. 63 comma 3 della Legge n. 231 del 21 novembre 2007:

- c) Ricettazione (art. 648 c.p.)*
- d) Riciclaggio (art. 648 bis c.p.).*
- e) Impiego di denaro, beni o utilità di provenienza illecita (art. 648 ter c.p.)*
- f) Antiriciclaggio*

2. LE AREE DI ATTIVITÀ A RISCHIO

In relazione a ciascuna delle tipologie di reati sopra descritte può delinearsi una specifica area a rischio.

Vengono qui descritte, sulla base di mere ipotesi di comportamenti delittuosi nell'ambito del processo aziendale di riferimento, le aree ritenute più specificamente a rischio:

- 1) Gestione delle transazioni finanziarie
- 2) Antiriciclaggio tributario

Per ognuna delle citate aree di attività ritenute a rischio sono stati identificati i processi aziendali e i controlli per ridurre il rischio dei comportamenti illeciti.

3. DESTINATARI DELLA PARTE SPECIALE

Destinatari della presente Parte Speciale sono gli amministratori, i dirigenti preposti alla redazione dei documenti contabili societari, rappresentanti e procuratori di VEGA, i sindaci, nonché il personale (dipendente e non) soggetto a vigilanza e controllo da parte dei soggetti apicali nelle aree di attività a rischio, qui di seguito tutti denominati "Destinatari".

Obiettivo della presente Parte Speciale è che tutti i Destinatari come sopra individuati, adottino regole di condotta conformi a quanto prescritto dalla stessa, al fine di impedire il verificarsi dei reati previsti nel Decreto.

4. PRESIDI DI CONTROLLO PRESCRITTI

La presente Parte Speciale prevede l'espresso divieto a carico dei Destinatari di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da integrare le fattispecie di reato sopra considerate (art. 25 octies del Decreto);
- porre in essere, collaborare o dare causa alla realizzazione di comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo.

Si evidenzia che rientrano tra le misure di prevenzione sempre applicabili:

- i principi comportamentali inseriti nel Codice Etico;
- i Principi di Controllo Generali indicati nella Parte Generale del presente Modello.

La presente Parte Speciale definisce, inoltre, i seguenti **Principi di Controllo Specifici** prevedendo:

- A) **procedure di approvvigionamento beni, lavori e/o servizi**: esistono strumenti normativi relativi al processo di approvvigionamento di beni, lavori e/o servizi che prevedono:

- trasparenza e identificazione dei ruoli: le norme aziendali sono ispirate, per ciascuna fase del processo di approvvigionamento, a criteri di trasparenza nei comportamenti e all'individuabilità dei soggetti responsabili del processo;
- modalità di approvvigionamento: esistono procedure che disciplinino la scelta della modalità di approvvigionamento da adottare (fornitore unico, utilizzo di vendor list qualificate, ecc);
- in caso di appalto, che si tenga conto dei requisiti tecnico-professionali degli appaltatori, ivi inclusi i requisiti di carattere generale, morale e di onorabilità e che si definiscano ruoli, responsabilità e modalità di monitoraggio sul rispetto delle normative di salute, sicurezza e igiene da parte dei fornitori nonché sulle attività da questi effettuate nei confronti dei sub-appaltatori in merito al rispetto delle suddette normative;
- modello di valutazione delle offerte: esiste un modello di valutazione delle offerte (tecniche/economiche) improntato alla trasparenza ed alla maggiore limitazione possibile di criteri di soggettività;
- approvvigionamenti in condizioni di urgenza: sono chiaramente definite le condizioni di urgenza in relazione alle quali si può commissionare direttamente la fornitura e devono essere definiti adeguati strumenti autorizzativi e di monitoraggio (report sottoposti ad adeguato livello gerarchico);
- Conservazione documentazione: deve esistere uno strumento normativo che indichi le modalità di archiviazione della documentazione relativa alla fornitura;

B) Deve esistere il divieto di:

- intrattenere rapporti, negoziare e/o stipulare e/o porre in esecuzione contratti o atti con persone indicate nelle **Liste di Riferimento** o facenti parte di organizzazioni presenti nelle stesse;
- concessione di utilità a persone indicate nelle **Liste di Riferimento** o facenti parte di organizzazioni presenti nelle stesse;
- assumere persone indicate nelle **Liste di Riferimento** o facenti parte di organizzazioni presenti nelle stesse.

- 20bis Deve essere adottato e attuato uno **strumento normativo** che annoveri:
 - la verifica preventiva dei presupposti di carattere strategico, economico e finanziario nonché dell'attuabilità della proposta di investimento da parte di un organo/unità
 - la verifica preventiva dei requisiti di onorabilità e professionalità dei partner commerciali/finanziari;
- C) E' adottata e attuata una **normativa antiriciclaggio** che è conforme alle applicabili disposizioni vigenti in materia e che annovera:
- il divieto di utilizzo del contante o altro strumento finanziario al portatore, per qualunque operazione di incasso, pagamento, trasferimento fondi, impiego o altro utilizzo di disponibilità finanziarie, nonché il divieto di utilizzo di conti correnti o libretti di risparmio in forma anonima o con intestazione fittizia;
 - il divieto di effettuare pagamento nel caso non esiste l'identità fra destinatari dei pagamenti e controparti effettivamente coinvolte nelle transazioni ad eccezione dei casi dove tale situazione non sia regolamentata da accordi documentabili;
 - l'obbligo di:
 - utilizzare operatori finanziari abilitati per la realizzazione di ciascuna delle operazioni di cui alla precedente lettera a);
 - inserire nelle clausole contrattuali la richiesta dell'attestazione sulla provenienza non delittuosa del denaro, dei beni, o delle altre utilità oggetto di trasferimento, sostituzione e/o impiego in attività economico/finanziarie;
 - utilizzare esclusivamente, nell'ambito della gestione delle transazioni finanziarie, operatori che attestano di essere muniti di presidi manuali e informatici e/o telematici atti a prevenire fenomeni di riciclaggio.



*Modello di organizzazione, gestione e controllo – aggiornamento 2016
ex decreto legislativo 8 giugno 2001, n. 231*

Se in via eccezionale un'attività aziendale, per un qualunque motivo, non è gestita secondo le previsioni dei presidi specifici di controllo di cui sopra, è comunque necessario il verificarsi contemporaneo delle seguenti condizioni :

- autorizzazione formale: esiste un'autorizzazione formalizzata preventiva di un Dirigente incaricato allo svolgimento dell'attività in oggetto, con evidenza e motivazione della ricorrenza del caso eccezionale, nonché. modalità operative, limiti, vincoli e responsabilità;
- reportistica: sono predisposti e archiviati verbali/report inviati al superiore gerarchico e da questo validati, dettagliati per ogni singola operazione nonché, ove applicabile, con descrizione delle modalità di gestione delle risorse finanziarie, relativi documenti giustificativi e attestazione di inerenza e congruità dell'operazione.

Rappresentano strumenti di presidio per VEGA:

- il regolamento acquisti beni, servizi e forniture
- il regolamento sui limiti di spesa del Comune di Venezia e linee di indirizzo



*Modello di organizzazione, gestione e controllo – aggiornamento 2016
ex decreto legislativo 8 giugno 2001, n. 231*

REATI AMBIENTALI

(ART. 25 UNDECIES)

1. LA TIPOLOGIA DEI REATI PREVISTI DALL'ART. 25 UNDECIES DEL DECRETO

Per quanto concerne la presente Parte Speciale si provvede di seguito a fornire una elencazione dei reati in essa contemplati, indicati nell'art. 25 undecies del Decreto introdotto dal d.lgs. n. 121 del 7 luglio 2011.

- uccisione, distruzione, cattura, prelievo, detenzione di esemplari di specie animali o vegetali selvatiche protette (art. 727-bis c.p.);
- distruzione o deterioramento di habitat all'interno di un sito protetto (art. 733-bis c.p.);
- scarichi di acque reflue industriali contenenti sostanze pericolose; scarichi sul suolo, nel sottosuolo e nelle acque sotterranee; scarico nelle acque del mare da parte di navi od aeromobili (D.Lgs 152/06, art. 137);
- attività di gestione di rifiuti non autorizzata (D.Lgs 152/06, art. 256);
- inquinamento del suolo, del sottosuolo, delle acque superficiali o delle acque sotterranee (D.Lgs 152/06, art. 257);
- violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (D.Lgs 152/06, art. 258);
- traffico illecito di rifiuti (D.Lgs 152/06, art. 259);
- attività organizzate per il traffico illecito di rifiuti (D.Lgs 152/06, art. 260);
- false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti nella predisposizione di un certificato di analisi di rifiuti; inserimento nel SISTRI di un certificato di analisi dei rifiuti falso; Omissione o fraudolenta alterazione della copia cartacea della scheda SISTRI - area movimentazione nel trasporto di rifiuti (D.Lgs 152/06, art. 260-bis);
- importazione, esportazione, detenzione, utilizzo per scopo di lucro, acquisto, vendita, esposizione o detenzione per la vendita o per fini commerciali di specie protette (L. 150/92, art. 1 e art. 2);
- Inquinamento doloso provocato da navi (D.Lgs. 202/07, art. 8);

- Inquinamento colposo provocato da navi (D.Lgs. 202/07, art. 9);

2. LE AREE DI ATTIVITA' A RISCHIO

In relazione a ciascuna delle tipologie di reati sopra descritte **sono state individuate le seguenti aree di attività a rischio:**

1. Acquisizione e/o cessione di asset (anche mediante acquisto e/o cessione di partecipazioni societaria di controllo) in relazione ai quali insistono obblighi ambientali;
2. Realizzazione, esercizio, modifica e/o dismissione di asset in relazione ai quali insistono obblighi ambientali in capo all'ente;
3. Gestione degli adempimenti e delle attività connessi alla bonifica, a seguito di un evento che sia potenzialmente in grado di contaminare il suolo, il sottosuolo, le acque superficiali e/o le acque sotterranee (limitatamente a serbatoi gasolio, gruppi elettrogeni con riferimento alle batterie di UPS per gruppo di continuità informatica);
4. Gestione delle emissioni atmosferiche (limitatamente a gruppi elettrogeni e caldaie);
5. Gestione delle sostanze lesive dell'ozono (limitatamente al sistema di condizionamento e perdite freon).

3. DESTINATARI DELLA PARTE SPECIALE

Destinatari della presente Parte Speciale sono gli amministratori, i dirigenti, rappresentanti e procuratori di VEGA, i sindaci, nonché il personale (dipendente e collanotori) soggetto a vigilanza e controllo da parte dei soggetti apicali nelle aree di attività a rischio, qui di seguito tutti denominati "Destinatari".



Modello di organizzazione, gestione e controllo – aggiornamento 2016
ex decreto legislativo 8 giugno 2001, n. 231

Obiettivo della presente Parte Speciale è che tutti i Destinatari come sopra individuati siano precisamente consapevoli della valenza dei comportamenti censurati e che quindi adottino regole di condotta conformi a quanto prescritto dalla stessa, al fine di impedire il verificarsi dei reati previsti nel Decreto

4. PRESIDI DI CONTROLLO PRESCRITTI

La presente Parte Speciale prevede l'espresso divieto a carico dei Destinatari di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da integrare le fattispecie di reato sopra considerate (art. 24-decies del Decreto);
- porre in essere, collaborare o dare causa alla realizzazione di comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo.

Si evidenzia che rientrano tra le misure di prevenzione sempre applicabili:

- i principi comportamentali inseriti nel Codice Etico;
- i Principi di Controllo Generali indicati nella Parte Generale del presente Modello.

La presente Parte Speciale definisce, inoltre, i seguenti **Principi di Controllo Specifici** prevedendo:

A) **Politica e Obiettivi**: esiste un documento formalizzato di Politica che definisca gli indirizzi e gli obiettivi generali in tema di ambiente, salute, sicurezza e igiene sul lavoro che l'azienda stabilisce di raggiungere e che:

- è formalmente approvato dalla direzione aziendale;
- contiene l'impegno ad essere conforme con le vigenti leggi in materia di salute, sicurezza e igiene applicabili e con gli altri requisiti sottoscritti;
- è adeguatamente diffuso ai dipendenti ed alle parti interessate;
- è periodicamente riesaminato per assicurare che gli obiettivi in esso indicati siano appropriati e adeguati rispetto ai rischi presenti nell'organizzazione (ad

es. riesame sulla base delle Linee Guida per l'attuazione del sistema di gestione della sicurezza, ambiente, dei nuovi regolamenti e delle leggi, etc.).

B) Norme e documentazione del sistema di gestione: deve essere adottato e attuato uno strumento normativo e/o organizzativo che:

- disciplini ruoli e responsabilità nella gestione della documentazione relativa al sistema di gestione della salute, della sicurezza, dell'ambiente e dell'incolumità pubblica (es. Manuale, Procedure, Istruzioni di lavoro) in coerenza con la Politica e le linee guida aziendali;
- definisca le modalità di gestione, archiviazione e conservazione della documentazione prodotta (es: modalità di archiviazione/protocollazione a garanzia di un adeguato livello di tracciabilità /verificabilità);
- disciplina ruoli e responsabilità dell'aggiornamento delle informazioni riguardo alla legislazione rilevante e alle altre prescrizioni applicabili in tema di salute, sicurezza e igiene sul lavoro;
- definisce criteri e modalità da adottarsi per la comunicazione degli aggiornamenti alle aree aziendali interessate.

C) Consultazione e comunicazione: è adottato e attuato uno strumento normativo e/o organizzativo che prevede riunioni periodiche di tutte le figure competenti per la verifica della situazione nella gestione delle tematiche riguardanti ambiente, salute, sicurezza e igiene e di una adeguata diffusione delle risultanze delle riunioni all'interno dell'organizzazione.

D) Diffusione delle informazioni, formazione, sensibilizzazione e competenze: è adottato e attuato uno strumento normativo e/o organizzativo che disciplini la diffusione delle informazioni previste dalla normativa vigente relative all'ambiente, salute, sicurezza e igiene. In particolare tale norma definisce:

- ruoli, responsabilità e modalità di informazione/formazione periodica delle funzioni competenti verso i lavoratori, in relazione alle tematiche ambiente, salute, sicurezza e igiene applicabili alle loro attività;
- l'informativa del Medico Competente, laddove necessario, relativamente ai processi e rischi connessi all'attività produttiva;
- i criteri di erogazione della formazione di ciascun lavoratore (es. all'assunzione, trasferimento o cambiamento di mansioni, introduzione di nuove attrezzature, tecnologie, sostanze pericolose);
- l'ambito, i contenuti e le modalità della formazione in dipendenza del ruolo assunto all'interno della struttura organizzativa;

E) **Rapporti con fornitori e contrattisti – clausole contrattuali, informazione e coordinamento:** deve essere adottato e attuato uno strumento normativo e/o organizzativo che definisca:

- ruoli, responsabilità e modalità di inserimento delle clausole contrattuali standard riguardanti il rispetto delle normative di ambiente, salute, sicurezza e igiene applicabili, nonché i costi della sicurezza nei contratti di somministrazione dei lavoratori, di appalto e di subappalto;
- ruoli, responsabilità, modalità e contenuti dell'informazione da fornire alle imprese esterne sui rischi specifici esistenti nell'ambiente in cui le imprese stesse sono destinate a operare e sulle misure da adottare in relazione alla propria attività che un'impresa appaltatrice aggiudicataria deve conoscere, impegnarsi a rispettare e a far rispettare ai propri dipendenti;
- ruoli, responsabilità e modalità di elaborazione del documento di valutazione dei rischi che indichi le misure da adottare per eliminare i rischi dovuti alle interferenze tra i lavoratori nel caso di diverse imprese coinvolte nell'esecuzione di un' opera.

F) **Gestione degli asset:** è adottato e attuato uno strumento normativo e/o organizzativo che disciplina le attività di manutenzione/ispezione degli asset

aziendali (es. attrezzature e impianti meccanici, elettrici ed elettromeccanici) affinché ne sia sempre garantita l'integrità e l'adeguatezza in termini di ambiente, salute e sicurezza dei lavoratori. In particolare tale norma:

- definisce ruoli, responsabilità e modalità di gestione degli asset;
- prevede periodiche verifiche di adeguatezza e integrità degli asset e di conformità ai requisiti normativi applicabili;
- prevede la pianificazione, effettuazione e verifica delle attività di ispezione e manutenzione tramite personale qualificato e idoneo.

G) **Sistema di deleghe di funzioni:** deve esistere un sistema di deleghe di funzioni tale da garantire, in capo al soggetto delegato, la sussistenza:

- di poteri decisionali coerenti con le deleghe assegnate;
- di potere di spesa adeguato, per l'efficace adempimento delle funzioni delegate;
- di un obbligo di rendicontazione formalizzata sui poteri delegati, con modalità prestabilite atte a garantire un'attività di vigilanza senza interferenze

H) **Controllo operativo:** deve essere adottato e attuato uno strumento normativo che, laddove necessario e con riferimento ai **compiti specifici conferiti**, individui i criteri e le modalità definite per l'affidamento dei compiti ai lavoratori in tema di ambiente, salute, sicurezza e igiene sul lavoro. In particolare tale norma:

- definisce ruoli, responsabilità e criteri di affidamento dei compiti ai lavoratori in tema di ambiente;
- definisce le misure organizzative per la partecipazione delle funzioni preposte nella definizione di ruoli e responsabilità dei lavoratori;
- prevede la tracciabilità delle attività di assessment svolte a tale scopo (es. definizione di check list mirate quali elenchi dei compiti critici e/o processi a impatto sull' ambiente).

- I) **Identificazione degli aspetti ambientali** e valutazione della loro significatività in funzione degli impatti ambientali diretti e indiretti ad essi correlati: deve essere adottato e attuato uno strumento normativo che identifichi ruoli, responsabilità, modalità operative, criteri e periodicità per la redazione e/o aggiornamento e l'approvazione dei documenti di identificazione:
- degli aspetti ambientali in funzione dei beni prodotti, dei servizi resi e delle attività svolte in condizioni operative normali, anomale, in condizioni di avviamento e di fermata e in situazioni di emergenza e di incidenti e la valutazione della loro significatività in funzione degli impatti ambientali diretti e indiretti ad essi correlati (sulla base, anche, del contesto territoriale di riferimento, nel rispetto della normativa vigente e delle prescrizioni previste nei relativi provvedimenti autorizzativi);
 - delle misure di prevenzione, protezione e mitigazione degli impatti ambientali conseguenti alla valutazione della significatività degli aspetti ambientali.
- L) **Autorizzazioni ambientali:** deve essere adottato e attuato uno strumento normativo che disciplini le attività di ottenimento, modifica e/o rinnovo delle autorizzazioni ambientali affinché siano svolte in osservanza alle prescrizioni normative vigenti.
- M) **Misura e monitoraggio delle prestazioni:** deve essere adottato e attuato uno strumento normativo e/o organizzativo che definisca ruoli, responsabilità, modalità e criteri per l'esecuzione delle attività di:
- identificazione e aggiornamento dei punti di scarico/emissione e dei punti di campionamento;
 - definizione del programma dei campionamenti e delle analisi degli scarichi/emissioni in linea con quanto previsto dalle prescrizioni autorizzative e dalla normativa vigente;
 - monitoraggio dei dati riguardanti gli scarichi/emissioni, ivi compresi i certificati delle analisi e i campionamenti effettuati.

N) **Trattamento dei superamenti dei valori limite autorizzati e azioni correttive:** deve essere adottato e attuato uno strumento normativo che definisca ruoli, responsabilità, modalità e criteri per l'esecuzione delle attività di:

- investigazione interna dei superamenti rilevati dalle determinazioni analitiche effettuate su scarichi/emissioni;
- risoluzione dei superamenti rilevati dalle determinazioni analitiche effettuate su scarichi/emissioni.

O) **Gestione degli asset contenenti sostanze lesive dell'ozono:** deve essere adottato e attuato uno strumento normativo che disciplini le attività di manutenzione/ispezione degli asset aziendali contenenti sostanze lesive dell'ozono. In particolare, tale strumento deve prevedere modalità e criteri per:

- il censimento degli asset contenenti sostanze lesive dell'ozono e la definizione del relativo piano dei controlli manutentivi e/o di cessazione dell'utilizzo e dismissione dell'asset, secondo quanto previsto dalla normativa vigente;
- le verifiche periodiche di rispetto del piano ed attivazione di azioni risolutive in caso di mancato rispetto.