

# Modello di organizzazione, gestione e controllo

in applicazione del  
Decreto Legislativo 8 Giugno 2001, n. 231, recante  
la “Disciplina della responsabilità amministrativa delle persone giuridiche,  
delle società e delle associazioni anche prive di personalità giuridica,  
a norma dell’art. 11 della legge 29 Settembre 2000, n. 300”

## Indice

	<u>Pagina</u>
1. IL DECRETO LEGISLATIVO N. 231/2001	3
1.1. Finalità e Enti interessati	3
1.2. Soggetti destinatari	3
1.3. Sanzioni	4
2. LA FONDAZIONE CENTRO NAZ.LE DI RICERCA IN HPC, BD E QC	5
2.1. Inquadramento giuridico e Scopo della Fondazione	5
2.2. Inquadramento organizzativo della Fondazione	6
2.3. Obiettivi e Finalità perseguiti con l’adozione del Modello	7
2.4. Approvazione, recepimento e modifiche del Modello	9
3. PARTE GENERALE DEL MODELLO	11
3.1. I principi generali di controllo a cui è ispirato il Modello	11
3.2. Protocollo relativo alla gestione economico-finanziaria	11
3.3. l’Organismo di Vigilanza	13
3.4. Reporting verso l’Organismo di Vigilanza	16
3.5. Responsabilità dell’Organismo di Vigilanza	17
3.6. Regole per la gestione del <i>Wistleblowing</i>	17
3.7. Formazione ed informazione del personale	18
3.8. I Referenti interni	19
3.9. Sistema disciplinare	19
4. REATI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE E TRA PRIVATI	21
4.1. Finalità, Documenti e Norma di riferimento	21
4.2. Principi generali di comportamento	22
4.3. Potenziali aree di attività a rischio	23
4.4. Gestione degli omaggi e delle ospitalità in ingresso ed in uscita	24
4.5. Acquisto di beni e servizi	24
4.6. Finanziamenti/contributi pubblici	24
4.7. Rapporti con gli enti pubblici competenti nei settori fiscale-tributario, previdenziale, tutela ambientale, sicurezza ed igiene sul lavoro	25
4.8. Autorizzazioni, licenze e concessioni amministrative	25
4.9. Accordi con clienti (c.d. Ciclo attivo) o fornitori (c.d. Ciclo passivo)	26
4.10. Selezione e assunzione del personale	26
4.11. Rapporti con banche/finanziarie/creditori	27
4.12. Conferimento di incarichi consulenziali/professionali	27
4.13. Attività ispettiva e di impulso dell’OdiV	27

## Indice

(segue)

		<u>Pagina</u>
5.	REATI INFORMATICI E TRATTAMENTO ILLECITO DEI DATI	28
	5.1. Quadro di riferimento	28
	5.2. Reati informatici identificati dal Decreto	28
	5.3. Potenziali attività a rischio	29
	5.4. Situazione Tecnico-organizzativa generale	32
	5.5. Tracciamento degli accessi esterni	33
	5.6. Accesso a risorse Interne	33
	5.7. Principali procedure da implementare	34
6.	REATI IN MATERIA DI TUTELA DELLA SALUTE E SICUREZZA SUL LAVORO (SSL)	37
	6.1. Le tipologie dei reati di omicidio colposo e lesioni gravi o gravissime	37
	6.2. Potenziali Aree di attività a Rischio	38
	6.3. Principi di comportamento	39
	6.4. Principi procedurali specifici	40
	6.5. Individuazione dei requisiti legali in materia di SSL	42
	6.6. Informazione, formazione ed addestramento	42
	6.7. Comunicazione, partecipazione e consultazione	44
	6.8. Monitoraggio e riesame	45
	6.9. I contratti di appalto	46
	6.10. Applicazione del modello e OdV	48
7.	REATI SOCIETARI	49
	7.1. Quadro di riferimento	49
	7.2. Reati societari identificati dal Decreto	49
	7.3. I processi sensibili	50
	7.4. I principi generali di comportamento	51
	7.5. I controlli dell'Organismo di Vigilanza	52
8.	REATI DI RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITA' DI PROVENIENZA ILLECITA	54
	8.1. Quadro di riferimento	54
	8.2. Potenziali attività a rischio	54
	8.3. Principi generali di comportamento	55
	8.4. I controlli dell'Organismo di Vigilanza	56
9.	REATI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE	58
	9.1. Quadro di riferimento	58
	9.2. Reati identificati nel Decreto e potenziali attività a rischio	59
	9.3. Potenziali Aree di attività a Rischio	60
	9.4. Principi generali di comportamento	61
	9.5. I controlli dell'Organismo di Vigilanza	64
10.	REATI AMBIENTALI	65
	10.1. Le tipologie dei reati ambientali	65
	10.2. Potenziali aree a rischio	66
	10.3. Principi generali di comportamento e attuazione	67
	10.4. Principi procedurali specifici	67
	10.5. Istruzioni e verifiche dell'Organismo di Vigilanza	68
11.	IMPIEGO DI LAVORATORI IRREGOLARI	69
	11.1. Reati inerenti all'impiego di lavoratori irregolari	69
	11.2. Potenziali aree a rischio	69
	11.3. Principi generali di riferimento	70
	11.4. I controlli dell'Organismo di Vigilanza	71

*Approvato dal Consiglio di Amministrazione  
del.....*

## 1. IL DECRETO LEGISLATIVO N. 231/2001

### 1.1. Finalità e Enti interessati

Il Decreto Legislativo 8 Giugno 2001, n. 231 - recante la “Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell’art. 11 della legge 29 Settembre 2000, n. 300” (di seguito “Decreto”) - ha introdotto per la prima volta nel nostro paese una forma di responsabilità dei soggetti collettivi definita “amministrativa”, nei fatti ritenuta dai più penale, per la commissione di certi reati espressamente previsti nel Decreto, posti in essere da soggetti apicali o dipendenti/collaboratori, a vantaggio o nell’interesse dell’ente stesso.

I soggetti collettivi destinatari della normativa sono:

- le persone giuridiche (enti ed associazioni forniti di personalità giuridica), ivi comprese le fondazioni, le società di capitali (piccole, medie o grandi che siano) e quelle cooperative;
- gli enti (società di persone ed associazioni) anche sprovvisti di personalità giuridica;
- gli enti pubblici che agiscono iure privatorum.

### 1.2. Soggetti destinatari

La definizione di due distinti rapporti funzionali (posizione apicale e posizione subordinata) è determinante per l’individuazione del criterio di imputazione soggettiva della responsabilità diretta ed autonoma dell’ente; in particolare, ai sensi dell’art. 5 del Decreto:

- per *soggetti apicali* il legislatore intende le persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell’ente o di una sua unità organizzativa, dotata di autonomia finanziaria e funzionale, nonché quelle persone che esercitano, anche di fatto, la gestione e il controllo dell’ente; a titolo esemplificativo: i legali rappresentanti, gli amministratori, i direttori generali, i direttori di stabilimento;
- per *dipendenti/collaboratori* il legislatore intende tutti coloro che sono sottoposti alla direzione o al controllo dei soggetti collocati in posizione apicale.

Se il reato è commesso da un soggetto in posizione apicale, si ha una responsabilità tendenzialmente assoluta (dolosa) dell’ente, con un’inversione dell’onere probatorio che risulta a carico dell’ente stesso; viceversa, in caso di reato perpetrato da un soggetto sottoposto all’altrui direzione, si ha una responsabilità della Fondazione per colpa, senza inversione dell’onere della prova, a carico quindi della pubblica accusa.

L'ente può essere ritenuto responsabile del reato commesso dai soggetti menzionati, a condizione che:

- l'ente non abbia preventivamente adottato ed efficacemente attuato un *Modello di organizzazione, gestione e controllo* (di seguito "Modello"), idoneo a prevenire reati del tipo di quello in concreto verificatosi;
- i fatti di reato siano stati posti in essere nel suo interesse o a suo vantaggio; la differenza sta nel fatto che la prima ipotesi concerne la finalizzazione soggettiva della condotta, ed è valutabile dal giudice penale in una prospettiva *ex ante*, antecedente o concomitante la commissione dell'illecito, mentre la seconda assume connotati più marcatamente oggettivi – potendo l'ente trarre un vantaggio anche nell'ipotesi in cui la persona fisica non abbia agito nel suo interesse – e richiede una verifica giudiziale da compiersi a fatto compiuto (*ex post*).

In generale, la responsabilità dell'ente sussiste solamente per quei reati (consumati o anche solamente tentati) espressamente previsti dagli artt. 24, 25 e ss. del Decreto, a cui si rimanda in quanto sempre oggetto di aggiornamento da parte degli organi competenti.

### 1.3. Sanzioni

Le sanzioni irrogate dal giudice, qualora venga accertata la responsabilità dell'ente in relazione al reato commesso, possono essere:

- *pecuniarie*; per espresso dettato legislativo, vengono commisurate alla gravità del reato commesso, al grado di corresponsabilità dell'ente, all'attività da esso svolta per eliminare o attenuare le conseguenze del fatto e per prevenire la commissione di ulteriori illeciti; vengono, infine, fissate sulla base delle condizioni economiche e patrimoniali dell'ente "allo scopo di assicurare l'efficacia della sanzione";
- *interdittive*; per menzionarne alcune, vanno dall'interdizione dall'esercizio dell'attività, alla sospensione o alla revoca delle autorizzazioni, licenze, o concessioni, al divieto di contrattare con la pubblica amministrazione, all'esclusione da agevolazioni, finanziamenti, contributi o sussidi, compresa l'eventuale revoca di quelli già concessi.

Sono, inoltre, previste la confisca del prezzo, del profitto ovvero di somme di denaro, beni o altre utilità di valore equivalente al prezzo o al prodotto del reato, e la pubblicazione della sentenza.

## 2. LA FONDAZIONE CENTRO NAZIONALE DI RICERCA IN HPC, BD E QC

### 2.1. Inquadramento giuridico e scopo della Fondazione

La Fondazione – costituita l’11 giugno 2022 da 51 Membri fondatori rappresentati da Università statali e non, Organismi di ricerca pubblici e non ed altri soggetti pubblici e privati - risponde ai principi e allo schema giuridico della fondazione di partecipazione, nell’ambito del più vasto genere di fondazioni disciplinato dal Codice Civile e leggi collegate, ed è soggetta alla disciplina di cui all’art. 14 e seguenti del Codice Civile; non persegue fini di lucro, né diretto né indiretto, e non può distribuire utili.

La Fondazione si pone come “organismo di diritto privato” in quanto, seppure caratterizzata dall’assenza di fini di lucro e di ripartizioni di utili tra i Membri:

- svolge attività economica finalizzata a conseguire le risorse necessarie al perseguimento dello scopo istituzionale;
- raccoglie contributi finanziari da una pluralità di soggetti, di natura pubblica e privata;
- si rapporta con il mercato dei fornitori di lavori, beni o servizi ponendo in essere procedure di acquisto trasparenti, imparziali e finalizzate a beneficiare della massima concorrenza nel mercato, secondo specifici regolamenti operativi approvati dal Consiglio di Amministrazione, avendo anche riferimento alle disposizioni del Codice dei Contratti Pubblici recato dal D.Lgs. 31.3.2023, n. 36 e smi.

La Fondazione ha come scopo la ricerca scientifica e tecnologica con riferimento a simulazioni, calcolo e analisi dei dati ad alte prestazioni (High-performance computing, Big data e Quantum computing), incluse le relative applicazioni in ogni ambito disciplinare e le relative ricadute nel contesto socio-economico, idonee a generare redditività economica secondo criteri di mercato. La Fondazione, dunque, realizza lo scopo di coniugare e temperare ricerca di base e ricerca applicata, capace di generare ritorni economici nel breve periodo ed applicazioni della ricerca valutabili secondo criteri di mercato, atte a contribuire alla sostenibilità economica della Fondazione.

In tale ambito - ai sensi dell’art. 5 del Decreto Direttoriale (DD) del Ministero dell’Università e della Ricerca (di seguito “MUR”) n. 3138 del 16.12.2021 e ss.mm.ii. - la Fondazione rappresenta il referente unico per l’attuazione del Programma di Ricerca finanziato dal PNRR, Missione 4, Componente 2, Investimento 1.4 (di seguito “Programma”), con specifico riferimento alla tematica suddetta; per gli anni di durata del PNRR, essa ne svolge le attività di gestione e di coordinamento, riceve le tranche di agevolazioni concesse da destinare alla realizzazione del suddetto programma, verifica e trasmette al MUR la rendicontazione delle attività svolte, potrà svolgere le attività di supporto trasversale previste dal medesimo DD, svolge ogni attività, anche strumentale, ritenuta dal Consiglio di Amministrazione necessaria,

utile o opportuna per la realizzazione del Programma e per assicurare l'adempimento delle previsioni dell'art. 15 del DD.

In termini più ampi, nello spirito del Programma il Centro Nazionale ha il ruolo di federare e coordinare le risorse di calcolo più significative del Paese nel dominio High Performance Computing (HPC), Big Data (BD) and Quantum Computing (QC), allo scopo precipuo di:

- rendere disponibile il potenziale di ricerca e innovazione in materia,
- costruire un ecosistema che sia globalmente attrattivo,
- rafforzare la competitività del Paese e contribuire alla leadership europea.

La Fondazione intende assolvere tale ruolo strategico:

- moltiplicando le opportunità per i partner e gli stakeholder, aumentando le capacità produttive in materia, e massimizzando l'impatto socio-economico nell'ambito di un ambiente di cooperazione diffusa; e
- realizzando qualcosa che oggi non esiste nel Paese, senza sovrapporsi o competere con le singole Istituzioni di ricerca già presenti, ma creando valore aggiunto per i propri partner e per la società nel suo insieme.

Dunque, per il raggiungimento delle proprie finalità istituzionali, anche oltre la durata del Programma di Ricerca CN-PNRR, la Fondazione svolge attività finalizzate alla:

- (i) creazione e/o al rinnovamento/ammodernamento di infrastrutture e laboratori di ricerca,
- (ii) realizzazione e allo sviluppo di programmi e attività di ricerca anche con il coinvolgimento di soggetti privati,
- (iii) realizzazione e allo sviluppo di programmi di formazione, a favorire la nascita e la crescita di iniziative imprenditoriali a più elevato contenuto tecnologico (start-up innovative e spin off da ricerca), e alla divulgazione e valorizzazione dei risultati della ricerca.

## 2.2. Inquadramento Organizzativo della Fondazione

Organi della Fondazione - definiti nell'art. 6 e segg. dello Statuto, a cui si rimanda per la descrizione delle competenze - sono:

- il Presidente (art. 13),
- il Consiglio di Amministrazione (art. 7 e segg.),
- l'Assemblea dei Membri della Fondazione (art. 15),
- il Collegio Sindacale (art. 17),
- il Direttore (art. 14).

A supporto del Consiglio di Amministrazione sono, inoltre, costituiti i seguenti Comitati consultivi (art. 16 dello Statuto):

- il *Board di Coordinamento degli Spoke*, con funzione di coordinamento degli Spoke in merito alle attività del Programma di ricerca CN-PNRR;

- l'*Industrial Advisory Board*, con funzione di consulenza sugli indirizzi strategici ed operativi della fondazione;
- l'*International Advisory Board*, con funzione di consulenza sulla pianificazione scientifica e sull'impatto delle attività di ricerca.

Il Consiglio di Amministrazione ha, ulteriormente, costituito i seguenti Comitati consultivi:

- l'*Ethics e Data Governance Board*, con funzioni consultive indipendenti, guida e feedback al Centro Nazionale in materia di etica e gestione dei dati;
- il *Comitato per l'Accesso al Supercomputing*, con funzione di valutazione delle richieste di accesso alle infrastrutture di calcolo e relativa allocazione delle risorse, secondo l'Access Policy approvata dal Consiglio di Amministrazione.

L'articolazione organizzativa della Fondazione è schematicamente espressa nell'Organigramma presentato in Allegato.

In termini di regolamento della funzionalità generale della Fondazione, sono stati finora predisposti i seguenti documenti, costituenti la base fondamentale per lo svolgersi delle attività della Fondazione:

- a) Statuto
- b) Codice Etico
- c) Regolamento sui conflitti d'interesse
- d) Regolamento per affidamento di servizi e forniture
- e) Regolamento per affidamento incarichi di consulenza
- f) Regolamento per i rimborsi spese di missione
- g) Regolamento per la selezione del Personale dipendente

### 2.3. Obiettivi e finalità perseguiti con l'adozione del Modello

Al di là delle esigenze e delle funzionalità organizzative correnti della Fondazione - progressivamente formalizzate in relazione allo sviluppo evolutivo delle attività svolte - il presente documento è stato redatto in applicazione del Decreto, allo scopo precipuo di istituire formalmente un'efficace e ragionevolmente agile struttura di regole, procedure e norme comportamentali che disciplinino l'organizzazione e la gestione della Fondazione e che costituiscano il *Modello di organizzazione, gestione e controllo* della medesima secondo le norme di legge (artt. 6 e 7 del Decreto), e delle indicazioni provenienti dalla dottrina giuridica, nonché dalla prassi giurisprudenziale in materia; esso ha i seguenti contenuti:

- procedure interne e standards di controllo con riferimento alle attività giudicate a rischio di reato;
- sistema disciplinare;
- Organismo di Vigilanza (di seguito OdiV) e sistema di *reporting* da e verso l'Organismo di Vigilanza;
- comunicazione e formazione.

Il Modello, se adottato ed efficacemente attuato, rappresenta per la Fondazione un efficace scudo protettivo; in effetti:

- se adottato prima della commissione dell'illecito permette di escludere totalmente la responsabilità dell'ente (secondo il linguaggio penalistico il Modello, in questa circostanza, è una causa di esclusione della colpevolezza dell'organismo collettivo) per il reato commesso dalla persona fisica funzionalmente ad esso legata (in questo caso, perciò, sarà solo il responsabile persona fisica a venire sottoposto a giudizio);
- se adottato dopo la commissione dell'illecito:
  - nel caso di irrogazione di *sanzioni pecuniarie*, determina una notevole riduzione delle medesime;
  - nel caso di irrogazione di sanzioni interdittive, esse non si applicano qualora vengano adottati comportamenti "virtuosi" quali il risarcimento del danno e/o la messa a disposizione del profitto, l'allontanamento dell'autore dell'illecito;
- nel caso di adozioni di misure cautelari interdittive durante la fase delle indagini preliminari, l'adozione del Modello comporta la sospensione delle medesime (sempre in presenza dei suddetti comportamenti "virtuosi").

I principi e le disposizioni enunciati nel presente documento trovano applicazione nei confronti di membri fondatori, amministratori, dipendenti e di chiunque operi per conto della Fondazione in virtù di un rapporto di natura contrattuale, di qualsivoglia tipologia, anche temporaneo, nei limiti dei propri compiti e delle responsabilità ad essi connesse.

La Fondazione, adottando un Modello adeguato alle prescrizioni del Decreto, evidenzia formalmente che opera in condizioni di correttezza e di trasparenza nella conduzione degli affari e delle attività. L'adozione del Modello rappresenta uno strumento di sensibilizzazione nei confronti di tutti i dipendenti e di tutti gli altri soggetti interessati da vicino alla realtà della Fondazione (ad es.: fornitori, clienti, collaboratori, consulenti), affinché tengano, nell'espletamento delle proprie attività, comportamenti corretti e lineari, tali da prevenire i rischi di reato esistenti.

In particolare, la Fondazione, attraverso l'adozione del Modello, si propone di:

- determinare, in tutti coloro che lavorano in suo nome e per conto, e soprattutto in coloro che operano nelle aree di attività risultate a rischio di reato, la consapevolezza di poter incorrere - in caso di violazioni delle disposizioni riportate nel Modello - nella commissione di illeciti passibili di sanzioni penali nei loro stessi confronti e di sanzioni "amministrative" irrogabili alla Fondazione;
- rendere consapevoli i predetti soggetti che tali comportamenti illeciti sono condannati con forza dalla Fondazione, in quanto gli stessi sono sempre e comunque contrari, oltre che alle disposizioni di legge, anche ai principi etici assunti come proprie linee guida nell'attività della Fondazione;
- consentire alla Fondazione di intervenire tempestivamente per prevenire o contrastare la commissione dei reati (elencati nella parte speciale del Decreto), o quanto meno di ridurre sensibilmente il danno da essi prodotto;
- favorire un significativo livello qualitativo in termini di trasparenza della governance e dell'immagine della Fondazione.

In estrema sintesi, la Fondazione conferma lo svolgimento della propria attività al rispetto dei valori e dei principi contenuti nel Modello e nel Codice Etico, nella

convincimento che la conduzione degli affari non possa distaccarsi dall'etica, condannando in particolare il ricorso a comportamenti illegittimi o comunque scorretti - pratiche corruttive, in ogni forma - allo scopo di raggiungere i propri obiettivi.

L'attività finalizzata alla predisposizione del Modello si è concretizzata:

- nella identificazione di settori, attività e aree sensibili nell'ambito della struttura e delle funzioni della Fondazione, con riferimento ai reati richiamati dal Decreto; *in considerazione della fase iniziale di organizzazione della Fondazione e del prevedibile sviluppo nel prossimo futuro verso stati di maggiore complessità organizzativa, tale identificazione è stata fatta in ottica evolutiva e non limitatamente allo stato presente al momento dell'approvazione iniziale di questo documento;*
- nell'esame analitico delle aree sensibili, con prefigurazione delle modalità e degli strumenti attraverso i quali la Fondazione, i suoi organi amministrativi, i dipendenti e, in generale, tutte le diverse figure contemplate dall'art. 5 del Decreto, potrebbero commettere i reati elencati nel Decreto medesimo;
- nell'individuazione delle procedure e dei protocolli esistenti - siano essi formalizzati o meno - in riferimento alle sole aree individuate come a rischio di reato;
- nella definizione di standards di comportamento e di procedure di controllo in relazione alle attività che si è ritenuto opportuno regolamentare;
- nella disciplina delle modalità di gestione delle risorse finanziarie idonee ad impedire la commissione di reati;
- nell'individuazione dei soggetti incaricati di vigilare sulla concreta applicazione del Modello, con contestuale predisposizione del relativo regolamento e sistema di reporting da e verso l'OdiV stesso;
- nella verifica del Codice Etico;
- nella previsione di un sistema disciplinare idoneo a sanzionare sia il mancato rispetto delle misure indicate nel Modello, sia le violazioni del Codice Etico.

Peraltro ogni valutazione del Modello riguarda la sua idoneità a minimizzare e non a escludere tout court la realizzazione di uno dei reati elencati nella parte speciale del Decreto da parte dei singoli soggetti.

#### 2.4. Approvazione, recepimento e modifiche del Modello

Il Modello, in conformità al disposto dell'art. 6 comma I, lettera a, del Decreto, è un atto di emanazione del Consiglio di Amministrazione e costituisce uno strumento con ambito di applicazione e finalità specifici, in quanto mira a prevenire la commissione dei reati previsti nel Decreto; esso, dunque, integra e non sostituisce gli strumenti organizzativi e di controllo nonché le procedure comportamentali operanti e quelli di futura emissione.

Il Consiglio di Amministrazione della Fondazione - anche su impulso dell'OdiV - provvederà ad effettuare successive modifiche ed integrazioni del Modello, del Codice Etico e del sistema disciplinare, allo scopo di consentire la continua rispondenza del Modello alle prescrizioni del Decreto ed all'evoluzione delle attività e della conseguente struttura organizzativa e gestionale della medesima.

Le attività di modifica ed integrazione del Modello devono essere compiute nel rispetto delle singole funzioni all'interno della Fondazione, con le quali restano necessari i confronti conclusivi sulla gestione delle specifiche procedure operative e degli standards di comportamento.

Il sistema di gestione per la prevenzione dei reati è costituito da una gerarchia di documenti, che necessitano di essere approvati e periodicamente aggiornati dal Consiglio di Amministrazione della Fondazione; in sintesi, tale gerarchia di documenti costituenti il Modello è:

- 1) Il Codice etico,
- 2) Parte generale del Modello,
- 3) Parti speciali del Modello (procedure comportamentali),
- 4) Modulistica (es. Schede di evidenza; moduli per audit).

### 3. PARTE GENERALE DEL MODELLO

#### 3.1. I principi generali di controllo a cui è ispirato il Modello

Il Modello di cui si dota la Fondazione riflette la sua peculiare soggettività giuridica, composta in un continuo equilibrio tra natura prettamente privatistica e natura pubblicistica.

Se da una parte è il Consiglio di Amministrazione della Fondazione a prendere decisioni relativamente all'attuazione del Modello - mediante valutazione ed approvazione delle azioni necessarie per l'implementazione degli elementi costitutivi dello stesso - l'attività di controllo sull'adeguatezza ed attuazione del Modello è di competenza dell'OdiV.

I principi di base utilizzati per improntare il Modello sono i seguenti:

- divisione fra potere e responsabilità di governance, direzione generale, direzione operativa, responsabilità di singole attività o progetti;
- definizione dell'organizzazione e delle funzioni interne, con individuazione nominale del personale di cui al punto precedente;
- delegabilità dei poteri solo nei limiti posti dall'organizzazione;
- assenza di svolgimento di compiti e funzioni di fatto senza legittimazione formale degli stessi;
- tracciabilità dell'iter decisionale ed esecutivo delle attività svolte, con massimo utilizzo di tecniche informatiche di comunicazione, per la massima rapidità dei rapporti interni,
- controllo e verifica delle attività compiute con reportistica adeguata.

#### 3.2. Protocollo relativo alla gestione economico-finanziaria della Fondazione

Di seguito sono sintetizzate le procedure di riferimento per la gestione ed il controllo.

##### 3.2.1. Gestione della liquidità

L'utilizzo della *Fondo Cassa contanti* - attivato al massimo su base fissa di € 100 - è solo per spese urgenti, di importo unitario inferiore a € 50, giustificate da Ordini di Acquisto e documenti giustificativi quali fatture, scontrini e ricevute.

I *conti correnti bancari* della Fondazione hanno, come Responsabili con potere di firma dispositivo, il Presidente e il Direttore: sono movimentati mediante registrazioni in contabilità di fatture passive e attive e, in generale, di:

- *bonifici in entrata*, di cui si ha notizia certa mediante la consultazione costante dei movimenti in tempo reale, presenti nell'home banking,
- *bonifici in uscita*, disposti dai Responsabili con poteri di firma, in base agli inserimenti sull'home banking operati dall'Ufficio Contabilità, come di seguito specificato.

Tutti i documenti sono firmati o dal Legale rappresentante o dai Procuratori Speciali.

Le *carte di credito/debito/bancomat* della Fondazione sono nominative. La riconciliazione tra l'estratto conto delle carte di credito e le spese sostenute avviene mediante la registrazione in contabilità della documentazione consegnata dal personale e/o ricevuta dal fornitore. Sono riconosciute solo le spese legate alla attività lavorativa.

### 3.2.2. Fatturazione passiva

Quando il personale della Fondazione riscontra la necessità di acquistare/noleggiare beni o servizi deve provvedere alla compilazione dell'apposita Proposta di Acquisto fornendo eventuale preventivo del fornitore proposto, che deve essere autorizzata dal Responsabile del settore.

L'Ufficio Acquisti (ovvero l'Addetto/a agli acquisti) prima di predisporre ed inoltrare al fornitore l'ordine di acquisto, ha il compito di verificare l'opportunità/esigenza di richiedere offerte a più fornitori, per un'adeguata valutazione comparativa.

Al ricevimento delle fatture elettroniche – eventualmente anticipate delle copie c.d. “di cortesia” – l'Ufficio Contabilità:

- provvede ad ottenere attestazione interna di conformità con quanto ordinato, da parte dei destinatari dei beni/servizi acquistati;
- verifica la corrispondenza del prezzo fra ordine e fattura;
- imposta il bonifico nel sistema di home banking in uso, per le successive disposizioni esecutive dei Responsabili con poteri di firma;
- archivia le copie cartacee, con l'evidenza dell'avvenuto pagamento, in raccoglitori suddivisi per mese, trasmessi allo Studio di Commercialisti che provvede alle registrazioni contabili.

### 3.2.3. Fatturazione attiva

La fatturazione attiva – sostanzialmente inesistente nel periodo del PNRR per la stessa natura dell'attività svolta - sarà prodotta a partire dai dati inseriti nell'apposita anagrafica clienti scaturente da ordini, contratti e convenzioni sottoscritti. Nel sistema saranno inserite tutte le offerte inviate ai clienti, che, qualora accettate e sottoscritte, saranno trasformate in contratti; la trasformazione prevederà l'inserimento di rate contenenti la data prevista di fatturazione, la competenza, l'importo e la descrizione del servizio.

Ciascun contratto sarà associato ad una commessa con un responsabile che autorizzerà la fatturazione della rata, al termine dei lavori in caso di servizi a progetto o alla data prevista se specificata nel contratto.

L'Ufficio Contabilità provvederà, quindi, a fatturare automaticamente tutte le rate che sono state autorizzate dai diversi responsabili.

### 3.2.4. Responsabilità nella gestione spese

Il *Direttore*, o suo delegato, è responsabile di:

- approvare le spese di beni e servizi e di lavori, beni e servizi in economia;
- decidere di effettuare eventuali visite presso la sede del fornitore, in base alla criticità del fornitore stesso per la realizzazione del prodotto finale;
- approvare le Relazioni tecniche predisposte per proporre l'acquisizione di nuovi beni e servizi, la cui spesa necessita dell'approvazione del Consiglio di Amministrazione;
- approvare gli Ordini di acquisto da inoltrare ai fornitori, tramite apposizione di firma,
- proporre l'inserimento di nuovi fornitori critici relativamente ai diversi settori che, man mano, saranno organizzati;
- comunicare all'Ufficio Acquisti i nominativi dei referenti di Proposte di Acquisto, da abilitare all'inserimento delle Proposte di Acquisto ed alla visualizzazione del budget.

Il *Consiglio di Amministrazione* è responsabile di approvare con delibera le spese per le quali non vigono deleghe al Presidente o al Direttore.

L'*Ufficio Acquisti* è responsabile di:

- gestire tutte le "Proposte di Acquisto" inserite dai proponenti;
- predisporre un elenco degli Ordini di acquisto da presentare al Direttore per la successiva approvazione;
- evadere gli ordini d'acquisto al fornitore, previa firma del Direttore, mediante compilazione ed invio dell'Ordine di Acquisto;
- provvedere agli acquisti urgenti di piccola entità, autorizzati previamente dal Direttore; provvedere all'archiviazione della documentazione relativa agli approvvigionamenti di propria competenza;
- inserire in anagrafica i nuovi fornitori;
- contattare il fornitore in caso di non conformità su forniture non critiche per l'immediata risoluzione della non conformità.

Il *Referente della Proposta di Acquisto* è responsabile di:

- compilare le "Proposta di Acquisto" e sottoporle all'approvazione del Direttore;
- effettuare il controllo in accettazione della merce, nel caso sia anche il Responsabile della valutazione dell'ordine.

### 3.3. L'Organismo di Vigilanza (OdiV)

Ai sensi dell'art. 6 comma I, lett. b) del Decreto, l'OdiV è organo dell'ente, dotato di autonomi poteri di iniziativa e di controllo, e deve vigilare sul funzionamento, l'efficacia, e l'osservanza del Modello, nonché curarne il costante e tempestivo aggiornamento.

In mancanza di indicazioni dettagliate fornite dal Decreto - in merito alla struttura e alla composizione di tale organismo - la decisione sui profili dei suoi componenti, secondo un'opinione condivisa, è rimessa al libero e responsabile apprezzamento degli enti.

La Fondazione opta per un OdiV collegiale, ritenendo tale scelta la più adeguata allo scopo a cui il suddetto organismo è preposto; pertanto, il Consiglio di Amministrazione nomina per questo incarico tre esperti, con competenze di natura giuridica, contabile, organizzativa e gestionale, effettivamente terzi rispetto ai soggetti che rivestono ruoli c.d. apicali e a coloro che prestano la loro opera nell'ambito delle aree operative da sottoporre a vigilanza.

Tuttavia, in considerazione della situazione di progressiva organizzazione della Fondazione, a partire da una catena di comando molto breve e di una complessità operativa molto limitata, il primo OdiV è monocratico, con prevalenti competenze giuridico-amministrative e caratteristiche di indipendenza come sopra delineate.

In particolare:

- per i membri dell'OdiV valgono le medesime cause di ineleggibilità e di decadenza che sussistono, ai sensi dell'art. 2399 c.c., per i componenti del Collegio sindacale;
- i componenti dell'OdiV non devono essere stati sottoposti a procedimento penale né condannati con sentenza (anche non passata in giudicato) per uno dei reati di cui al Decreto;
- la cessazione dall'incarico per scadenza del termine avrà effetto dal momento in cui è stato formato il nuovo OdiV;
- gli esperti che compongono l'OdiV possono essere revocati dal Consiglio di Amministrazione solo per giusta causa; la revoca deve essere deliberata, previa audizione degli interessati;
- l'OdiV può essere riconfermato per non più di tre mandati consecutivi; ogni mandato ha la durata di tre anni;
- in caso di cessazione, revoca, morte, rinuncia o decadenza dei componenti dell'OdiV, il Consiglio di Amministrazione è obbligato a provvedere tempestivamente alla nomina del nuovo OdiV;
- all'OdiV è attribuito dal Consiglio di Amministrazione, sin dall'atto di nomina, autonomia finanziaria, nel rispetto del budget della Fondazione, al fine di effettuare spese necessarie al corretto funzionamento dello stesso;
- la retribuzione dell'OdiV viene determinata dal Consiglio di Amministrazione all'atto della nomina per l'intero periodo di durata dell'ufficio.

L'OdiV svolge le seguenti attività:

- vigilanza sull'effettività del Modello, verificando in particolare la coerenza tra il Modello medesimo e le concrete procedure adottate nelle aree a rischio;
- verifica periodica del rispetto del Modello da parte di tutte le singole unità/aree della Fondazione a rischio, allo scopo di accertare che le procedure definite ed i presidi approntati siano seguiti nel modo più fedele possibile e risultino in concreto idonei a prevenire i rischi della commissione dei reati evidenziati;
- vigilanza affinché il Codice etico e tutte le disposizioni in esso contenute siano rispettate da tutti i soggetti a qualsiasi titolo operanti nella Fondazione;
- formulazione di proposte di aggiornamento e modifica del Modello agli organi competenti, in collaborazione con le funzioni all'interno della Fondazione

coinvolte, nel caso in cui mutate condizioni e/o normative ne comportino, a suo giudizio, necessità di aggiornamento e/o implementazione.

In particolare, l'OdiV, come sopra individuato:

- cura l'aggiornamento del Modello, in conformità alle evoluzioni della legge e della giurisprudenza, oltre che in conseguenza di modifiche intervenute nell'organizzazione della Fondazione;
- collabora con le varie funzioni all'interno della Fondazione interessate alla predisposizione ed integrazione della normativa interna (regole di comportamento, istruzioni operative, eventuali manuali di controllo) volta alla prevenzione dei rischi di reato mappati;
- vigila sul corretto funzionamento delle attività di controllo per ciascuna area a rischio, segnalando tempestivamente anomalie e disfunzioni del Modello, previo confronto con le aree/funzioni interessate;
- provvede a diffondere, con le modalità che ritiene più opportune, la conoscenza e la comprensione del Modello all'interno della Fondazione, prestando maggiore attenzione alle aree ritenute più esposte ai rischi di reato mappati (specificamente le aree/funzioni che si occupano della gestione delle risorse economiche, della contabilità, quelle che intrattengono rapporti con le pubbliche amministrazioni, la gestione della sicurezza e della salute sul lavoro);
- compie periodiche verifiche mirate su specifiche operazioni o atti posti in essere nell'ambito dei processi monitorati perché sensibili;
- dispone verifiche straordinarie laddove si evidenzino disfunzioni del Modello o si verifichi- o soltanto si abbia il sospetto che si possa verificare - la commissione di atti illeciti oggetto delle attività di prevenzione;
- effettua il monitoraggio dell'andamento delle attività a rischio, coordinandosi con le funzioni all'interno della Fondazione, anche tramite apposite riunioni;
- raccoglie, elabora e conserva le informazioni rilevanti in ordine al rispetto del Modello;
- redige periodicamente relazioni sull'adeguatezza e sull'efficacia del Modello, anche sulla base di quanto emerso dalle attività di verifica e controllo, trasmettendole al Consiglio di Amministrazione, al Collegio sindacale e all'Assemblea dei Membri fondatori;
- verifica periodicamente la praticabilità e l'attuazione delle eventuali soluzioni correttive alle procedure specifiche contenute nel Modello;
- valuta e propone l'irrogazione di eventuali sanzioni disciplinari, previo il necessario coordinamento con i responsabili delle competenti funzioni/aree della Fondazione.

Infine, l'OdiV:

- svolge la sua attività, salvo situazioni urgenti e casi particolari, con periodicità da definire a cura del Presidente dell'OdV.
- laddove lo ritenga necessario per lo svolgimento dei suoi compiti, dovrà poter interloquire con i vertici decisionali ed operativi della Fondazione.

Il rapporto tra la Fondazione e i componenti dell'OdV sarà regolato da apposito contratto, redatto per iscritto.

### 3.4. Reporting verso l'Organismo di Vigilanza

L'OdiV è destinatario di qualsiasi informazione, documentazione e comunicazione, proveniente anche da terzi, attinente al rispetto del Modello; esso definisce la documentazione che, su base periodica, deve essere sottoposta alla sua attenzione. All'OdiV debbono essere obbligatoriamente trasmessi:

- provvedimenti e notizie, provenienti da organi di polizia giudiziaria o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti per le fattispecie di reato previste dal Decreto, riguardanti la Fondazione;
- richieste di assistenza legale avanzate dai soggetti interni alla Fondazione, in caso di avvio di procedimenti giudiziari per i reati previsti dal Decreto;
- rapporti predisposti dalle strutture della Fondazione nell'ambito della loro attività di controllo, dai quali emergano elementi di criticità rispetto alle norme del Decreto;
- in via periodica, notizie relative all'effettiva attuazione del Modello in tutte le aree/funzioni a rischio della Fondazione;
- in via periodica, notizie relative all'effettivo rispetto del Codice Etico a tutti i livelli all'interno della Fondazione;
- informazioni sull'evoluzione delle attività attinenti le aree a rischio.

In caso di informazioni e notizie, anche ufficiose, relative alla commissione dei reati previsti dal Decreto o comunque riguardanti possibili violazioni del Modello (comprensivo delle disposizioni del Codice Etico) ciascuno deve rivolgersi al proprio Responsabile, il quale riferisce immediatamente all'OdiV.

Qualora la notizia di possibile commissione di reati o violazioni del Modello coinvolga il Consiglio di Amministrazione della Fondazione viene informato direttamente e solamente l'OdiV.

I flussi informativi devono pervenire all'OdiV per iscritto o attraverso l'utilizzo di una casella di posta elettronica appositamente dedicata. Le segnalazioni, eventualmente anche in forma anonima, aventi ad oggetto l'evidenza o il sospetto di violazione del Modello, devono essere il più possibile circostanziate.

L'OdiV:

- agisce in modo da garantire gli autori delle segnalazioni contro qualsiasi forma di ritorsione, discriminazione o penalizzazione, garantendo altresì la riservatezza della loro identità, fatti salvi gli obblighi di legge e la tutela dei diritti della Fondazione o delle persone accusate erroneamente o in malafede;
- valuta le segnalazioni ricevute e decide le azioni da intraprendere, ascoltando, se necessario, l'autore della segnalazione e il responsabile della presunta violazione.

Qualora l'autore dell'illecito dovesse essere il Presidente del Consiglio di Amministrazione, l'OdiV effettua una sommaria istruttoria, il cui esito viene trasmesso al Presidente del Collegio Sindacale che, effettuati gli approfondimenti necessari, assumerà i provvedimenti più opportuni, avendo cura di informare l'OdiV.

L'OdiV invia periodicamente una relazione sull'attività da esso svolta, e sul grado di attuazione del Modello, al Consiglio di Amministrazione e al Collegio Sindacale.

L'OdiV predispone un apposito archivio, anche in formato elettronico, in cui viene custodito ogni relazione, informazione, segnalazione ai sensi del presente documento, per un periodo di 10 anni. E' fatta salva l'osservanza delle disposizioni in materia di riservatezza dei dati personali e dei diritti da essa garantiti in favore degli interessati. L'accesso all'archivio è consentito esclusivamente ai membri dell'OdiV.

### 3.5. Responsabilità dell'Organismo di Vigilanza

In caso di commissione di illeciti da parte della Fondazione, a seguito del mancato esercizio del potere di vigilanza sull'attuazione e sul funzionamento del modello, l'OdiV potrebbe essere giudicato responsabile penalmente sulla base della disposizione contenuta all'art. 40, comma II, Codice Penale, dunque, del principio secondo cui "non impedire un evento, che si ha l'obbligo giuridico di impedire, equivale a cagionarlo".

Tuttavia, ad eccezione degli obblighi giuridici penalmente rilevanti, previsti in capo a tale organo dalla normativa antiriciclaggio, è ormai pacifico che non sia possibile ricostruire in capo all'OdiV una siffatta responsabilità in quanto tali posizioni di garanzia si fondano su espliciti poteri-doveri impeditivi e non sulla base di un generale dovere di sorveglianza, come è quello configurato per l'OdiV della Fondazione.

### 3.6. Regole per la gestione del Wistleblowing

Il D. Lgs. 24/2023 disciplina la protezione delle persone che segnalano violazioni di disposizioni normative nazionali o dell'UE, che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato di cui siano avvenute a conoscenza in un contesto lavorativo pubblico o privato (art. 1, comma).

L'articolo 4, comma 1, del decreto succitato obbliga gli enti destinatari di dotarsi di un proprio canale interno di segnalazioni di illeciti, il Wistleblowing, che garantisca la riservatezza dell'identità della persona segnalante, della persona coinvolta e della persona comunque menzionata nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione.

La Fondazione, nel rispetto del D.lgs. 24/2023, definisce che tali segnalazioni potranno avvenire:

- in forma scritta attraverso un box presente negli uffici della Sede, dove le segnalazioni saranno del tutto anonime;
- in forma scritta attraverso la casella di posta elettronica dell'OdiV che garantisce la riservatezza dell'identità del segnalante;
- in forma orale al proprio Responsabile.

L'OdiV prenderà in considerazione tutte le segnalazioni ricevute in forma scritta, comprese quelle anonime, nonché quelle orali ricevute dal Responsabile, e valuterà le eventuali conseguenti iniziative da intraprendere a sua ragionevole discrezione e responsabilità, ascoltando eventualmente l'autore della segnalazione e/o il responsabile della presunta violazione motivando per iscritto ogni relativa decisione assunta.

La Fondazione:

- richiede all'OdiV o al Responsabile che ha ricevuto la segnalazione di gestirla in maniera confidenziale, così da assicurare la riservatezza dell'identità del segnalante e di altre persone coinvolte o a cui si fa riferimento nella segnalazione, fatti salvi gli obblighi di legge e a tutela dei diritti della Fondazione o delle persone accusate erroneamente e/o in male fede;
- vieta rappresaglie e protegge coloro che fanno segnalazioni in buona fede da ritorsioni, discriminazioni o penalizzazioni, dirette o indirette, per motivi collegati alla segnalazione;
- garantisce che il personale sia a conoscenza delle procedure di segnalazione e sia in grado di usarle, essendo consapevole dei propri diritti e delle tutele nel quadro delle procedure adottate, attraverso idonea comunicazione;
- prevede, in caso di riscontrata violazione delle misure di tutela del segnalante, nonché di riscontrate segnalazioni infondate rivelate con dolo o colpa grave, ad indentificare e applicare la sanzione ritenuta più adeguata alla circostanza.

### 3.7. Formazione ed informazione del personale

La Fondazione intende garantire una corretta e completa conoscenza del Modello e del contenuto del Decreto, nonché degli obblighi derivanti dal medesimo.

La formazione e l'informativa è assicurata dal Presidente del Consiglio di Amministrazione coadiuvato dall'OdiV, in stretto coordinamento con i responsabili delle funzioni coinvolte nell'applicazione del Modello.

Tale sforzo formativo ed informativo è esteso anche a tutti quei soggetti che, pur non appartenendo alla Fondazione, operano comunque nell'interesse o a vantaggio della medesima; ai soggetti terzi è rivolta solamente l'attività di comunicazione e di formazione avente ad oggetto il Codice Etico. Nei contratti stipulati con i terzi saranno inserite clausole contrattuali standard, che impegnano gli stessi a non adottare comportamenti non in linea con i principi di condotta e con i valori etici cui si ispira la Fondazione.

L'attività di formazione continuativa e di aggiornamento è organizzata a cura dell'OdiV, facendo ricorso ad incontri periodici obbligatori, modulati nei contenuti e nella frequenza, in funzione della qualifica dei destinatari e della funzione dagli stessi ricoperta.

Se ritenuto necessario dall'OdiV, interverranno agli incontri professionisti esterni aventi specifiche competenze sul tema dei reati ascrivibili alla Fondazione, dell'analisi delle procedure e dei processi organizzativi, nonché dei principi generali sulla legislazione in materia di compliance e dei controlli ad essi correlati.

### 3.8. I Referenti interni

Per attività complesse possono essere designati dal Direttore specifici referenti interni, quali soggetti preposti alla regolare esecuzione di ciascuna operazione sensibile; essi costituiscono il primo presidio per scongiurare il rischio di commissione dei reati e sono, altresì, referenti diretti dell'OdiV per ogni attività informativa e di controllo. In particolare, i referenti interni al completamento dell'intero Modello:

- vigilano sul regolare svolgimento dell'operazione di cui sono referenti;
- informano collaboratori e sottoposti in merito ai rischi di commissione dei reati connessi alle attività svolte;
- per eventuali operazioni sensibili predispongono e conservano la documentazione rilevante e ne sintetizzano i contenuti per l'OdiV;
- comunicano all'OdiV le eventuali anomalie riscontrate, nonché qualsiasi altra circostanza rilevante ai fini della corretta applicazione del Modello;
- contribuiscono all'aggiornamento del sistema di controllo relativo alla propria area di appartenenza ed informano l'OdiV delle modifiche e degli interventi ritenuti opportuni;
- verificano l'esistenza di modalità di evidenza, solitamente di tipo informatico, curandone la struttura e gli eventuali successivi aggiornamenti.

### 3.9. Sistema disciplinare

Il sistema disciplinare di seguito delineato è applicabile in caso di violazioni delle procedure comportamentali indicate nel Modello, nonché dei principi e delle disposizioni stabiliti nel Codice Etico; esso costituisce un deterrente per la commissione degli illeciti penali per i quali scatta il meccanismo della responsabilità della Fondazione, ex Decreto.

L'instaurazione di un procedimento disciplinare e l'eventuale applicazione delle relative sanzioni non sono condizionati dall'instaurazione di un giudizio penale e dal suo esito; chi di competenza, infatti, possiede la facoltà di applicare, all'esito delle opportune valutazioni, le sanzioni che ritiene più adeguate al caso concreto, non dovendo le stesse, in virtù della loro autonomia, coincidere con le valutazioni e i convincimenti del giudice penale.

#### 3.9.1. Amministratori (non dirigenti) e Sindaci

In caso di violazione accertata del Modello (e quindi anche del Codice Etico) da parte di Amministratori o Sindaci, tale circostanza va denunciata senza indugio all'OdiV da chi la rileva.

Se la denuncia non è manifestamente infondata, l'OdiV ne informerà tempestivamente il Presidente del Consiglio di Amministrazione ed il Presidente del Collegio Sindacale (a patto che non siano i soggetti coinvolti nella violazione, nel qual caso la denuncia verrà fatta all'Amministratore e al Sindaco non coinvolti, più anziani di età), i quali provvederanno ad assumere le opportune iniziative previste dalla vigente normativa.

Si applicano le disposizioni di cui agli artt. 2392 e 2407 del codice civile nonché quelle di cui agli artt. 2383 terzo comma e 2400 secondo comma del codice civile.

### 3.9.2. Dirigenti (anche amministratori)

In caso di violazioni da parte di Dirigenti (anche amministratori) delle prescrizioni del presente Modello, nell'espletamento di attività nelle aree a rischio, si provvederà ad applicare nei confronti dei responsabili le misure più idonee in conformità a quanto previsto dal *C.C.N.L. dei Dirigenti delle Aziende del Terziario, Distribuzione e Servizi*, a cui la Fondazione aderisce.

### 3.9.3. Personale dipendente non dirigente

Le sanzioni disciplinari applicabili al personale dipendente, nei cui confronti è stata accertata la violazione delle regole e dei principi contenuti nel Modello, rientrano tra quelle previste dal *C.C.N.L. per le Aziende del Terziario, Distribuzione e Servizi*, a cui la Fondazione aderisce.

L'accertamento delle infrazioni, i procedimenti disciplinari e l'irrogazione delle sanzioni rientrano nelle competenze della Direzione della Fondazione.

Il provvedimento disciplinare non potrà essere applicato prima che siano trascorsi cinque giorni dalla contestazione per iscritto del fatto, nel corso dei quali la lavoratrice e il lavoratore potranno presentare le loro giustificazioni.

Trascorso il predetto termine, ove la Fondazione non abbia ritenuto valide le giustificazioni proposte, o in assenza di giustificazioni della lavoratrice o del lavoratore, la stessa potrà dare applicazione alle sanzioni disciplinari dandone motivata comunicazione all'interessato/a.

Se il provvedimento non verrà comunicato entro i dieci giorni successivi a quello della presentazione delle giustificazioni, le stesse si riterranno accolte.

Non può tenersi conto ad alcun effetto delle sanzioni disciplinari decorsi due anni dalla loro applicazione e parimenti l'arco temporale per l'individuazione del numero delle infrazioni e dei corrispondenti provvedimenti disciplinari è di due anni.

Il sistema disciplinare viene costantemente monitorato dall'OdiV.

### 3.9.4. Collaboratori, consulenti, fornitori e altri soggetti terzi aventi rapporti contrattuali con la Fondazione

Qualsiasi inosservanza delle regole comportamentali indicate nel Modello, da parte di collaboratori, consulenti, fornitori ed altri soggetti terzi, può determinare, conformemente a quanto disciplinato nello specifico rapporto contrattuale, la risoluzione del rapporto contrattuale, fatta salva la facoltà di richiedere il risarcimento dei danni verificatisi in conseguenza di tali comportamenti illeciti, ivi inclusi quelli derivati dall'applicazione da parte del giudice penale delle misure previste dal Decreto.

La competenza a valutare l'idoneità di questo genere di cautele è dell'OdiV, che cura anche l'eventuale aggiornamento delle precauzioni anzi descritte.

#### 4. REATI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE E TRA PRIVATI

##### 4.1. Finalità, Documenti e Norma di riferimento

Dalla ricognizione e valutazione dei processi e delle attività della Fondazione - considerati “sensibili” con riferimento ai reati contro la Pubblica Amministrazione (di seguito PA) e tra Privati, previsti dal Decreto – sono state raccolte informazioni al fine di fornire elementi utili all’identificazione del rischio e allo sviluppo di ipotesi di miglioramento:

- per ciascun reato è stata riportata la definizione ed una analisi delle aree coinvolte e dei ruoli di responsabilità in essa inclusi;
- dall’analisi dei processi e delle informazioni raccolte, sono state individuate le possibili condotte illecite e di conseguenza gli eventuali reati;
- è stato, inoltre, indicato, come previsto dal Decreto, il ruolo dei soggetti coinvolti distinguendo fra figure apicali e sottoposti;
- sono stati identificati e descritti i punti di controllo esistenti e ne è stata fornita valutazione rispetto alla mitigazione dei rischi individuati.

Questa parte del Modello si riferisce a comportamenti posti in essere da amministratori, dirigenti e dipendenti operanti nelle aree di attività a rischio, nonché da collaboratori esterni e partners; l’obiettivo è fare in modo che tali soggetti si attengano a regole di condotta conformi ai principi di seguito prescritti, al fine di prevenire il verificarsi di reati contro la PA e tra Privati.

In particolare, questa parte del Modello ha la funzione di:

- fornire un elenco dei principi generali, nonché dei principi procedurali specifici cui i soggetti, in relazione al tipo di rapporto in essere con la Fondazione, sono tenuti ad attenersi ai fini di una corretta applicazione del Modello;
- fornire all’OdiV ed ai referenti delle altre funzioni aziendali, chiamati a cooperare con lo stesso, gli strumenti operativi per la concreta attuazione del Modello e per il relativo esercizio delle attività di controllo, monitoraggio e verifica previste.

Nell’espletamento di tutte le attività rilevanti ai sensi del Modello, i soggetti interessati devono in generale conoscere e rispettare, con riferimento alle attività svolte, le regole ed i principi contenuti nei seguenti documenti della Fondazione:

- Statuto;
- Regolamenti adottati dal Consiglio di Amministrazione della Fondazione (per la disciplina dell’organizzazione e governo delle attività interne, degli incarichi e delle collaborazioni con persone fisiche esterne, delle esternalizzazioni ad operatori economici);
- Codice Etico;
- Regolamento per la disciplina dei conflitti d’interesse.

Per il testo integrale delle norme incriminatrici identificate nel Decreto si rimanda ai rispettivi articoli del Codice Penale; specificamente:

- Malversazione a danno dello Stato o di altro Ente Pubblico (art. 316 bis Codice Penale)
- Indebita percezione di erogazioni a danno dello Stato o di altro Ente Pubblico (art. 316 ter Codice Penale)
- Truffa aggravata a danno dello Stato o di altro Ente Pubblico (artt. 640 e 640 bis Codice Penale)
- Corruzione nelle sue varie declinazioni (artt. 318, 319, 319 ter, 322, 322 bis Codice Penale)
- Concussione (artt. 317 bis, 322 Codice Penale)
- Corruzione tra Privati (art. 2635 Codice Civile)

#### 4.2. Principi generali di comportamento

Nella Parte Generale di questo Modello sono già evidenziate una pluralità di situazioni potenzialmente a rischio, con relative indicazioni procedurali di comportamento, idonee a minimizzare il rischio del reato di corruzione; in generale, poi, valgono le indicazioni sulle politiche della Fondazione in materia, espresse nel Codice Etico.

In particolare, ai destinatari è fatto divieto di:

- ricevere, pretendere, corrispondere e offrire direttamente o indirettamente, compensi di qualunque natura, regali, vantaggi economici o altre utilità da/a un soggetto privato o ente da esso direttamente o indirettamente rappresentato che:
  - eccedano un modico valore e il limite di ragionevoli prassi di cortesia;
  - siano suscettibili di essere interpretati come volti a influenzare indebitamente i rapporti tra la Fondazione e il predetto soggetto o l'ente da esso direttamente o indirettamente rappresentato, a prescindere dalla finalità di perseguimento, anche esclusivo, dell'interesse o del vantaggio della Fondazione;
- corrispondere pagamenti di modico valore non ufficiali, effettuati allo scopo di velocizzare, favorire o assicurare l'effettuazione di un'attività di routine o, comunque, prevista nell'ambito dei doveri dei soggetti privati con cui la Fondazione si relaziona;
- utilizzare fondi o mezzi personali allo scopo di aggirare l'applicazione dei contenuti del presente Modello;
- sottoscrivere contratti superiori al valore soglia indicato nella procura specifica, ove non autorizzati per iscritto dai vertici.

Inoltre, ogni attività svolta nelle aree sensibili sopra indicate deve essere accuratamente e regolarmente riflessa nei documenti contabili, restando responsabilità primaria della Fondazione la redazione di documenti contabili che riflettano con un dettaglio ragionevole ciascuna operazione, nonché la definizione ed esecuzione di controlli adeguati al fine di garantire che:

- le operazioni siano effettive ed eseguite solo a fronte di un'autorizzazione dei soggetti delegati;

- le operazioni siano registrate al fine di permettere la redazione del bilancio in conformità con i principi contabili di riferimento;
- il valore dei beni inserito a bilancio sia riscontrato, con una certa periodicità, con gli inventari e siano adottate appropriate misure in riferimento alle differenze riscontrate.

Non è consentito imporre o accettare alcuna prestazione ove la stessa può essere realizzata solamente pregiudicando i valori ed i principi del Codice Etico o violando le procedure applicabili del Modello e le normative in vigore.

#### 4.3. Potenziali aree di attività a rischio

Di norma, le aree/attività più esposte a rischio di reati contro la P.A. (nazionale e non) sono quelle di seguito elencate:

- partecipazione a gare d'appalto,
- predisposizione di gare d'appalto,
- finanziamenti/contributi pubblici,
- rapporti con gli enti pubblici competenti nei settori fiscale-tributario, previdenziale, tutela ambientale, sicurezza ed igiene sul lavoro,
- autorizzazioni, licenze e concessioni amministrative.

Si rilevano, altresì, ancorché indirettamente, le seguenti attività:

- rapporti con clienti (c.d. Ciclo attivo) o fornitori (c.d. Ciclo passivo)
- selezione ed assunzione del personale,
- rapporti con banche/finanziarie/creditori
- gestione del contenzioso tributario/giudiziario,
- conferimento di incarichi consulenziali/professionali.

L'individuazione e la valutazione dei rischi-reati contro la P.A. o contro il Patrimonio pubblico sono operate anche in considerazione delle seguenti ragioni:

- i soggetti coinvolti (prevalentemente apicali) nelle aree/attività sopra elencate sono relativamente pochi ma dotati, specialmente nel caso del Presidente del Consiglio di Amministrazione e del Direttore, di poteri decisionali e di spesa limitati da quanto deliberato dal Consiglio di Amministrazione;
- il turn over delle figure coinvolte attivamente nelle attività a rischio è limitato;
- il personale della Fondazione – di per sé recentemente costituita - proviene da istituzioni pubbliche e private di solida cultura organizzativa;
- la Fondazione è dotata di Codice Etico specificamente rivolto anche alla prevenzione dei reati;
- in qualità di apicali e di dipendenti della Fondazione non risultano indagati e/o rinviati a giudizio per delitti contro la P.A. o contro il patrimonio pubblico;
- nelle attività/aree sensibili si osservano prassi dimensionate, pur senza procedure scritte ad hoc, tendenti a diminuire il rischio (anche soltanto indiretto e mediato) di commissione di delitti contro la P.A. o contro il Patrimonio Pubblico.

I principi comportamentali, i controlli in essere, la descrizione delle modalità di commissione dei reati, i principi procedurali e le indicazioni operative da adottare ed osservare che verranno indicate di seguito hanno lo scopo di contribuire ad arginare i rischi di reato rilevati.

#### 4.4. Gestione degli omaggi e delle ospitalità in ingresso e in uscita

E' vietato a tutto il personale della Fondazione ricevere, pretendere, corrispondere e offrire direttamente o indirettamente, compensi di qualunque natura, omaggi, vantaggi economici o altra utilità, inclusi i trattamenti di ospitalità, da/a un soggetto pubblico/privato che eccedano il modico valore, così come specificato nel Codice Etico, e comunque siano suscettibili di essere interpretati come volti ad influenzare indebitamente i rapporti tra la Fondazione e il predetto soggetto, a prescindere dalla finalità di perseguimento, anche esclusivo, dell'interesse o del vantaggio della Fondazione.

Sul tema si rimanda a quanto riportato nel punto 5.6 del Codice Etico della Fondazione, con particolare riferimento alla definizione di tipi e finalità degli omaggi e delle ospitalità, ai limiti di valore ed ai livelli autorizzativi necessari, alle regole di comportamento.

#### 4.5. Acquisto di beni e servizi

Il *Regolamento per l'affidamento di servizi e forniture*, approvato dal Consiglio di Amministrazione, ha l'obiettivo di definire le modalità operative, i controlli e le responsabilità coinvolte per la gestione delle attività di approvvigionamento della Fondazione; la procedura risponde all'esigenza di stabilire un protocollo standard e controlli definiti al fine di prevenire il rischio dei reati di corruzione (art. 318-319 c.p.) e di concussione (art. 317 c.p.).

#### 4.6. Finanziamenti/contributi pubblici

Con l'obiettivo di definire le modalità operative, i controlli e le responsabilità coinvolte per la gestione delle fasi di un progetto per ottenere finanziamenti e/o contributi pubblici, nazionali e non, dovrà essere definita una specifica procedura di supporto.

La procedura si applicherà al processo di partecipazione della Fondazione ad un progetto bandito da una Pubblica Amministrazione ed Enti Pubblici nazionali o comunitari; le attività oggetto della procedura saranno puntualizzate nelle seguenti 7 fasi:

1. descrizione del progetto,
2. esame del progetto,
3. istruzione della pratica,
4. presentazione del progetto,
5. gestione/rendicontazione/accreditamento contributi
6. gestione di eventuali obblighi e impegni del progetto finanziato,
7. archiviazione della documentazione.

Tale procedura risponde all'esigenza di definire un protocollo standard e controlli definiti al fine di prevenire il rischio dei reati di:

- malversazione a danno dello Stato (art. 316 - bis Codice Penale),
- indebita percezione di erogazioni a danno dello Stato (art. 316 - ter c.p.),
- truffa ai danni dello Stato (art. 640 c.p.), e
- corruzione (art. 318-319 c.p.).

I maggiori rischi penali sono legati a produzioni documentali false o all'invio di dati non veritieri o, ancora, all'assunzione di personale su accordo con i Pubblici Ufficiali/Incaricati di Pubblico Servizio.

#### 4.7. Rapporti con gli enti pubblici competenti nei settori fiscale-tributario, previdenziale, tutela ambientale, sicurezza ed igiene sul lavoro

A seconda degli ambiti e delle materie interessate dall'attività del singolo ente pubblico con funzioni di controllo - ad esempio, Inail, Inps, Agenzia dell'Entrate, ASL - la gestione del rapporto è affidata ai referenti interni per ciascun ambito/aspetto interessato dell'attività della Fondazione, ovvero ai consulenti esterni allo scopo coinvolti. Solitamente sono coinvolti il Consulente del Lavoro, lo Studio di Commercialista e il settore amministrativo della Fondazione in progressiva strutturazione.

La firma di eventuali dichiarazioni e/o documenti di qualsivoglia genere viene apposta dal Presidente o dal Direttore. E' opportuno che l'OdiV venga tempestivamente informato dei controlli e delle verifiche ispettive in programma o, comunque, da poco avviate.

Quanto sopra risponde all'esigenza di stabilire un protocollo standard e controlli definiti al fine di prevenire il rischio del reato di corruzione (art. 318-319 c.p.).

I maggiori rischi penali sono legati a produzioni documentali false o all'invio di dati non veritieri o, ancora, all'assunzione di personale su accordo con i Pubblici Ufficiali/Incaricati di Pubblico Servizio.

#### 4.8. Autorizzazioni, licenze e concessioni amministrative

I processi aventi ad oggetto i rapporti e le attività intrattenuti da personale della Fondazione per l'ottenimento di autorizzazioni, concessioni e licenze seguono prassi formali perlopiù definite dalle controparti a cui obbligatoriamente aderire.

La pratica di richiesta delle autorizzazioni, licenze e concessioni è, di norma, attivata a livello di segreteria di Presidenza/Direzione, inviandola alle controparti sotto la supervisione del Presidente/Direttore stesso.

La gestione di tali rapporti - caratterizzata da incontri tra personale della Fondazione e Pubblici Ufficiali e/o contatti telefonici - e il loro andamento, dalla fase iniziale fino a quella conclusiva, sono documentati al fine di consentire di ripercorrere l'intero processo.

I delitti di corruzione potrebbero essere perpetrati da soggetti apicali o comunque con ruoli dirigenziali dotati di potere di spesa per favorire o accelerare l'ottenimento di un'autorizzazione/concessione/licenza. Tale prassi evidenzia, dunque, l'esigenza

di definire un protocollo standard e controlli definiti al fine di prevenire il rischio del reato di corruzione (art. 318-319 c.p.).

I maggiori rischi penali sono legati a produzioni documentali false o all'invio di dati non veritieri o, ancora, all'assunzione di personale su accordo con i Pubblici Ufficiali/Incaricati di Pubblico Servizio.

#### 4.9. Rapporti con clienti (c.d. Ciclo attivo) o fornitori (c.d. Ciclo passivo)

All'interno del ciclo attivo e, in particolare, nell'esecuzione di prestazioni di servizi ad altra società, il reato di corruzione tra privati potrebbe essere commesso da parte degli organi apicali della Fondazione:

- con lo scopo di ottenere dal cliente la conclusione di un contratto;
- con lo scopo di corrompere un concorrente durante la partecipazione a una "gara privata" affinché lo stesso presenti condizioni peggiori.

Nel ciclo passivo, invece, il reato di corruzione potrebbe essere integrato nei confronti dei fornitori della Fondazione per ottenere beni/servizi a migliori condizioni e/o a prezzi più favorevoli per la controparte.

#### 4.10. Selezione ed assunzione del personale

L'assunzione del personale, essendo di natura altamente specialistica, viene effettuata nell'ambito dei singoli settori di competenza con la supervisione diretta del Presidente/Direttore della Fondazione.

La corruzione potrebbe essere commessa mediante l'assunzione da parte della Fondazione di persone a conoscenza di segreti industriali di Enti concorrenti al fine di ottenere la rivelazione di tali segreti.

I referenti dei diversi settori sostengono i colloqui con i soggetti proposti dalle società di recruitment incaricate o attraverso l'esame di curricula vitae presentati, in applicazione del *Regolamento per la selezione del personale* approvato dal Consiglio di Amministrazione. Dei colloqui effettuati sono redatti i verbali, con le conclusioni raggiunte, mantenuti dalla segreteria del Presidente/Direttore.

La segreteria del Presidente/Direttore predispone la lettera di assunzione/collaborazione, supervisionata e firmata dal Presidente o Direttore, secondo i rispettivi poteri attribuiti dal Consiglio di Amministrazione.

La suddetta procedura risponde all'esigenza di stabilire un protocollo standard e controlli definiti al fine di prevenire il rischio del reato di corruzione (art. 318-319 c.p.).

#### 4.1.1. Rapporti con banche/finanziarie/creditori

Il reato potrebbe essere commesso nei rapporti con le banche o società finanziarie, mediante la corruzione di funzionari per ottenere benefici economici o, comunque, benefici illeciti. Il reato di corruzione potrebbe integrarsi nei rapporti con i creditori con lo scopo di concludere transazioni più vantaggiose per la Fondazione ovvero al fine di ritardare l'azione esecutiva.

#### 4.1.2. Conferimento di incarichi consulenziali/professionali

Per gli incarichi consulenziali/professionali – inclusi quelli finalizzati alla gestione del contenzioso tributario/giudiziario - la Fondazione si affida a professionisti fidati, perlopiù individuati attraverso indagine di mercato, a seguito di necessità, per le capacità professionali di cui la Fondazione medesima è venuta a conoscenza.

Tali professionisti ricevono per iscritto la conferma dell'incarico da espletare, da cui risultano in modo chiaro i termini, le condizioni previste e apposite clausole finalizzate al rispetto della normativa del Decreto, del relativo Modello adottato dalla Fondazione (comprensivo di Codice Etico), con la previsione di una clausola che regoli le conseguenze della violazione del suddetto impegno (ad es.: clausole risolutive espresse, penali).

Gli originali della lettera di incarico, o del contratto, sono archiviati presso la segreteria del Presidente/Direttore che ha, altresì, cura di conservare i riscontri dell'attività svolta dal professionista, oltre che i pagamenti effettuati, nelle forme e con le modalità consentite dalla natura della prestazione resa. Non sono ammessi pagamenti in contanti ovvero rimborsi per spese non previste nella lettera di incarico. I passi operativi sono contenuti nel *Regolamento per l'affidamento degli incarichi di consulenza* approvato dal Consiglio di Amministrazione<sup>2</sup>.

Tale procedura risponde all'esigenza di definire un protocollo standard e controlli definiti al fine di prevenire il rischio del reato di corruzione (art. 318-319 c.p.).

#### 4.1.3. Attività ispettiva e di impulso dell'OdiV

Fermo restando quanto già previsto nella parte generale del Modello sull'OdiV, compiti ulteriori dell'Organo sono:

- segnalazione di necessità di aggiornamento di procedure operative o comportamentali finalizzate alla minimizzazione dei rischi di reato;
- verifica periodica, con il supporto delle altre funzioni competenti, del sistema di deleghe e procure in vigore, con raccomandazione di opportune modifiche nel caso in cui il potere di gestione o la qualifica non corrispondano ai poteri di rappresentanza conferiti ai referenti.

## 5. REATI INFORMATICI E TRATTAMENTO ILLECITO DEI DATI

### 5.1. Quadro di riferimento

La Legge n. 48 del 18/03/2008, che ratifica la Convenzione di Budapest del Consiglio d'Europa sulla criminalità informatica, introduce l'art. 24 bis nel Decreto inserendo così i reati informatici ed il trattamento illecito di dati fra i reati presupposto della responsabilità amministrativa dell'Ente. I reati relativi all'abuso della tecnologia informatica qui consideratisi sono quelli compiuti verso sistemi informatici e telematici (es.: danneggiamento di sistema informatico) e non l'utilizzo dell'elaboratore nella realizzazione del fatto (es.: frode informatica) ex art. 640 ter del Codice Penale.

Si distingue fra *sistema informatico* e *dato informatico* ai fini delle sanzioni applicabili: il danneggiamento di un sistema informatico può impedire in toto l'utilizzo del sistema mentre il danno ad un dato informatico (es.: un file) non comporta solitamente il mancato funzionamento di tutto il sistema. In base alla Convenzione di Budapest:

- con “*sistema informatico o telematico*” si intende una “*qualsiasi apparecchiatura, dispositivo, gruppo di apparecchiature o dispositivi, interconnesse o collegate, una o più delle quali, in base ad un programma, eseguono l'elaborazione automatica dei dati*”; in questo senso, data l'ampiezza della definizione, anche un unico PC collegato ad una rete ADSL, oppure un cellulare/palmare sono da considerarsi sistemi informatici;
- per “*dato informatico*” si intende una “*qualsiasi rappresentazione di fatti, informazioni o concetti in forma idonea per l'elaborazione con un sistema informatico, incluso un programma in grado di consentire ad un sistema informatico di svolgere una funzione*”.

Date, quindi, le caratteristiche dei reati informatici che risultano realizzabili con l'utilizzo degli strumenti che si utilizzano quotidianamente per l'attività lavorativa e dato il loro difficile accertamento, con questa parte del Modello la Fondazione mira a concretizzare alcuni fattori di deterrenza:

- sensibilizzare e formare il personale al fine di renderlo edotto e consapevole delle condotte che si configurano come reati informatici e delle relative sanzioni previste dall'ordinamento giuridico e dalla Fondazione;
- monitorare e conservare alcuni file di log dell'utilizzo degli strumenti informatici aziendali derivanti da necessità connesse alla sicurezza e produttività;
- definire regole comportamentali proceduralizzate, per l'utilizzo degli strumenti informatici aziendali e dei servizi Interni e di posta elettronica al fine di prevenire il verificarsi dei reati informatici.

### 5.2. Reati informatici identificati dal Decreto

L'art. 24 bis del Decreto classifica i reati informatici in tre diversi gruppi, attribuendo diversi livelli sanzionatori a livello pecuniario, fino ad arrivare a sanzioni interdittive dell'attività aziendale, anche in via preventiva cautelare:

- il primo comma dell'art. 24 bis considera i reati che hanno come fattore comune il "*danneggiamento informatico*" (hardware, software e dati);
- il secondo comma raggruppa due reati che puniscono *condotte prodromiche alla lesione dei beni giuridici tutelati* e cioè la mera detenzione abusiva di codici di accesso e programmi atti a danneggiare sistemi informatici e telematici;
- il terzo comma considera i reati relativi al *falso di un documento informatico* e la frode del soggetto che presta servizi di certificazione attraverso firma digitale.

Nel seguito si analizzeranno i seguenti articoli chiamati in causa nell'art. 24 bis, cercando di fornire esempi chiarificatori delle condotte punibili:

- Accesso abusivo ad un sistema informatico o telematico (art. 615 ter Codice Penale)
- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater c.p.)
- Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico (art. 615 quinquies c.p.)
- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater c.p.)
- Installazione di apparecchiature atte ad intercettare, impedire o 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 comunque 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.)
- Documenti informatici (art. 491 bis c.p.)
- Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 quinquies c.p.)

### 5.3. Potenziali attività a rischio

Considerando che i reati informatici si possono commettere con l'utilizzo di un PC, tutte le attività della Fondazione sono astrattamente a rischio, in quanto tutto il personale è dotato di desktop/laptop collegato alla intranet della Fondazione, ove attivata, ed alla rete Internet. Per una migliore comprensione delle potenziali aree di attività a rischio di commissione dei reati sopra riportati, sono di seguito spiegate, anche tramite casi esemplificativi, le principali fattispecie di reato.

#### 5.3.1. Danneggiamento di informazioni, dati e programmi informatici di privati (art. 635 bis c.p), dello Stato o di altri enti pubblici o di pubblica utilità (art. 635 ter c.p.)

Tali fattispecie di reato si realizzano quando un soggetto distrugge, deteriora, cancella o altera o sopprime informazioni, dati o programmi informatici altrui, di concorrenti oppure soggetti pubblici; un esempio è la condotta di chi moltiplica le connessioni contemporanee ad un sito-target al fine di rallentarne o impedirne l'attività.

La norma prevede un incremento della pena se il reato è commesso da un operatore di sistema, venendosi a trovare, data la sua particolare mansione, in una posizione di vantaggio - avendo con più facilità di accesso al sistema e ad aree riservate e di controllarne le operazioni - e potendo, quindi, con più facilità commettere il reato; tali tipologie di reato sono astrattamente possibili, anche se la loro effettiva realizzazione è stata valutata come improbabile date le procedure di selezione e di verifica dell'operato degli amministratori di sistema. L'art. 635 ter prevede una tutela rafforzata con pene più severe nel caso in cui i dati e le informazioni colpite siano pubblici o di pubblica utilità.

#### 5.3.2. Danneggiamento di sistemi informatici e telematici di privati (art. 635 quater del c.p) o di pubblica utilità (art. 635 quinquies de c.p.)

Tali fattispecie di reato prevedono pene più severe rispetto al semplice danneggiamento di dati o file in quanto tali condotte possono pregiudicare il funzionamento, totale o parziale, del sistema informatico; la condotta si realizza, ad esempio, diffondendo virus e altri programmi malevoli che compromettono od ostacolano seriamente l'utilizzo del sistema informatico.

#### 5.3.3. Accesso abusivo ad un sistema informatico o telematico (art. 615 ter c.p.)

Tale fattispecie di reato punisce chi si introduca abusivamente in un sistema informatico o telematico protetto da misure di sicurezza, a prescindere dalla qualità e robustezza di tali misure. La fattispecie punisce il semplice accesso abusivo, anche nel caso in cui all'accesso non segua un vero e proprio danneggiamento od utilizzo dei dati acceduti; è, quindi, sufficiente violare le misure di difesa del sistema informatico ed introdursi nel sistema, anche solo per visualizzare un documento, perché si configuri tale fattispecie di reato. Sempre di accesso abusivo si tratta nel caso in cui un dipendente accede ad informazioni nel sistema informatico aziendale protetto, senza esserne autorizzato.

La responsabilità della Fondazione si ha se da tale accesso abusivo - ad esempio in caso di introduzione in un sistema informatico di un concorrente - sia presente un interesse o vantaggio dell'ente a tale condotta. Per altro verso, l'eventuale accesso del datore di lavoro alla posta elettronica aziendale o alla postazione di lavoro assegnata al dipendente non è da considerarsi accesso abusivo secondo quanto chiarito dalla Giurisprudenza e dal Garante per la privacy.

#### 5.3.4. Detenzione e diffusione abusiva di codici di accesso e diffusione di programmi atti a danneggiare o interrompere un sistema informatico (art. 615 quater e 615 quinquies c.p.)

Tali fattispecie di reato hanno un carattere preventivo in quanto puniscono condotte preliminari all'accesso abusivo; è punita la semplice detenzione e diffusione abusiva di codici di accesso quali password di accesso a sistemi o dispositivi informatici quali badge o smart card. L'art. 615 quinquies punisce, invece, la diffusione di virus atti a danneggiare o interrompere un sistema informatico o telematico aziendale.

L'interesse o vantaggio dell'ente si ravvisa, ad esempio, ove il dipendente detenga abusivamente codici di accesso a sistemi informatici di una società concorrente allo scopo di controllare le attività del concorrente; per entrambe le fattispecie di reato

si ritiene che il rischio che si realizzino tali condotte nell'interesse o a vantaggio della Fondazione sia molto basso.

5.3.5. Intercettazione, impedimento o interruzione di comunicazioni e reati di installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 quater e 617 quinquies del c.p.)

Il reato di cui all'art. 617 quater del c.p. si configura quando un soggetto intercetti, impedisca od interrompa in maniera fraudolenta le comunicazioni di un sistema informatico o telematico, o intercorrenti tra più sistemi, e riveli il contenuto delle comunicazioni intercettate al pubblico mediante qualsiasi mezzo di informazione. E', infatti, possibile, tramite tecniche di intercettazione, prendere cognizione del contenuto delle comunicazioni, nel corso della trasmissione dei dati, e modificarne la destinazione al fine di violare la riservatezza della corrispondenza telematica o comprometterne l'integrità o impedirne l'arrivo a destinazione; è il caso, ad esempio, di un dipendente o soggetto apicale che impedisce una determinata comunicazione telematica del concorrente al fine di evitare che l'impresa concorrente invii la propria offerta di partecipazione ad una gara.

L'art. 617 quinquies punisce il reato di chi installa apparecchiature, fuori dai casi consentiti dalla legge, idonee ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche: la condotta si realizza, dunque, con la mera installazione di tali apparecchiature a prescindere poi dal fatto che vengano utilizzate o meno.

Il rischio connesso alle condotte di cui all'art. 617 quater e quinquies è valutato come molto basso.

5.3.6. Falso in un documento informatico pubblico o privato, avente efficacia probatoria (art. 491 bis c.p.)

Tale reato mira a tutelare la fede pubblica ovvero l'affidamento della collettività sulla genuinità di certi documenti e dei fatti in essi descritti.

Per documento informatico si intende, secondo il Codice dell'amministrazione digitale (D.lgs. n. 82 del 7 marzo 2005) come la "rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti"; la falsificazione di un documento può riguardare:

- la falsità materiale, che si ha, ad esempio, quando si falsifica la firma dell'autore o quanto si lede l'integrità del documento alterandolo per mezzo di aggiunte o cancellazione indebite in seguito alla sua formazione;
- la falsità ideologica, che riguarda i documenti pubblici (espressione dell'esercizio di funzione pubblica o pubblico servizio) e si ha quando un documento informatico non è veritiero, nel senso che pur non essendo stato contraffatto contiene delle dichiarazioni false.

In Fondazione i documenti informatici possono circolare liberamente quindi la fattispecie di falsificazione di un documento è astrattamente facilmente realizzabile;

tuttavia, nel caso si sospetti una violazione delle policy di accesso è possibile verificare i file di log, conservati in archivio, ad accesso ristretto agli amministratori di sistema incaricati.

#### 5.3.7. Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 quinquies c.p.)

Tale tipologia di reato è stata valutata come non applicabile alla Fondazione, in quanto non presta servizi di certificazione di firma elettronica.

#### 5.4. Situazione Tecnico Organizzativa generale

Il personale della Fondazione è dotato di un Postazione di Lavoro (PdiL) connessa alla rete Internet. L'accesso alla rete Internet è considerato uno strumento di lavoro, fornito dalla Fondazione per portare a compimento le diverse attività lavorative; il suo utilizzo deve, perciò, essere principalmente congruo a tali scopi; in nessun caso attività diverse da quelle lavorative devono avere conseguenze negative sulla Fondazione (ad esempio: utilizzo di risorse della Fondazione, costi da questo derivanti, rischi per la sicurezza delle informazioni e dei sistemi della Fondazione, danni causati a terzi) e, comunque, l'uso dell'accesso alla rete Internet deve sempre avvenire nel rispetto delle norme e leggi vigenti. La responsabilità in caso di eventi avversi derivanti da un suo uso improprio rimangono a totale carico dell'utilizzatore.

Dal punto di vista tecnico esistono, però, poche o nessuna limitazioni a ciò che il personale può compiere con tale dotazione, non avendo, per scelta della Fondazione, ristretto la navigazione in internet; in effetti, la natura delle attività svolte dal personale richiede la possibilità di accedere in modo ampio alle risorse ed ai servizi presenti in Internet. Per questo motivo, la navigazione e l'utilizzo dei servizi non sono ristretti per gli utilizzatori della rete, per tutto ciò che è direttamente collegato allo svolgimento degli incarichi ricevuti a qualunque titolo, direttamente o indirettamente, dalla Fondazione o comunque per tutte le attività che possono essere ricondotte al motivo per il quale è stato dato all'interessato accesso alla rete.

Dunque, l'impiego della propria PdiL per commettere reati informatici non può essere prevenuto utilizzando contromisure tecniche, restando il dipendente in grado di commettere reati informatici a danno di terzi esterni alla rete della Fondazione, utilizzando una postazione di lavoro della medesima, grosso modo come se stesse utilizzando propri strumenti. Situazione simile vale per i server di cui la Fondazione si doterà; in generale, essi saranno protetti da sistemi di firewall o packet filtering per quanto riguarda il traffico in ingresso mentre è consentito loro di accedere ad ogni risorsa in Internet, direttamente o per tramite di opportuni gateway.

Pertanto, ritenendo questa situazione indispensabile per il corretto svolgimento delle mansioni del personale e per l'erogazione dei servizi, la prevenzione dei reati informatici è basata, in questo senso non su misure tecnologiche "restrittive", bensì facendo leva sulla formazione e motivazione del personale e, come deterrente, sulla tracciabilità delle azioni compiute.

## 5.5. Tracciamento degli accessi esterni

Dal punto di vista della dissuasione e della capacità a posteriori di risalire al responsabile di una azione eventualmente delittuosa portata a termine attraverso la rete della Fondazione - *subordinatamente alla effettiva realizzazione di una siffatta rete proprietaria nei nuovi uffici del Tecnopolo di Bologna* - si intende realizzare un sistema di registrazioni elettroniche che consentano la tracciabilità delle azioni compiute da chi utilizza la rete. In particolare:

### 5.5.1. Postazioni di Lavoro individuali (PdiL)

Le registrazioni dovranno consentire, a partire dagli elementi identificativi di una connessione di rete (indirizzo IP e porta di destinazione, data e ora), di identificare:

- per l'accesso tramite rete cablata, l'indirizzo fisico della scheda di rete e la presa di distribuzione del cablaggio utilizzata per l'accesso alla rete; in tal modo, l'individuazione della persona che ha effettuato il collegamento è possibile solo se l'indirizzo della scheda di rete risulta censito e riconducibile a una PdiL fornita dalla Fondazione, restando tale prova sostanzialmente "indiziaria" in quanto è possibile mediante opportuni accorgimenti modificare l'indirizzo fisico della scheda di rete;
- per l'accesso tramite rete wireless, l'username col quale si è ottenuto l'accesso alla rete wireless; gli accessi wireless potranno essere differenziati, per i dipendenti e per gli ospiti, ognuno mediante username e password individuali, restando sempre possibile risalire all'identità dell'assegnatario delle credenziali di accesso.

### 5.5.2. Server della Fondazione

Il tracciamento a livello di rete, anche a causa del volume di traffico coinvolto, sarà svolto mediante campionamento del traffico, restando i server in genere dotati di indirizzo IP pubblico statico, per cui i parametri identificativi di una connessione di rete (ip/porta sorgente, ip/porta destinazione) permetteranno di risalire ad un singolo server.

La tracciabilità dipenderà, quindi, dalla possibilità che chi ha subito l'azione sia in grado di fornire l'indirizzo di provenienza della connessione di rete; poiché ogni server è un sistema multi utente, verosimilmente non saranno in generale mantenute tracce complete che consentano di individuare con certezza il responsabile, bensì saranno disponibili elementi di indagine che possano restringere notevolmente il campo di ricerca (ad esempio, l'elenco delle persone collegate al server in un determinato periodo, l'elenco dei programmi eseguiti). Tali registrazioni dovranno essere mantenute per almeno 6 mesi.

## 5.6. Accesso a risorse Interne

In termini generali, il personale della Fondazione - *subordinatamente alla effettiva disponibilità di una infrastruttura di calcolo dedicata nei nuovi uffici del Tecnopolo di Bologna* - potrà disporre per l'esecuzione delle proprie attività di:

- accessi a server della Fondazione contenenti dati di soggetti terzi, la cui violazione di integrità, confidenzialità o disponibilità può costituire un danno per il titolare del dato e quindi configurarsi come reato informatico;
- accesso anche fisico a server di proprietà di terzi ospitati presso la Fondazione;
- accesso a sistemi informativi esterni di proprietà di terzi sui quali la Fondazione potrebbe fornire servizi di varia natura.

Le misure di cui si prevede l'adozione sono, in breve, le seguenti:

- protezione fisica delle zone in cui sono contenuti i server della Fondazione, per mezzo di controllo degli accessi tramite badge, con relativa registrazione;
- accesso ai sistemi della Fondazione con credenziali individuali; utenze condivise saranno consentite solo a personale autorizzato, con registrazione dell'accesso in opportuni file di log, fatto salvo l'accesso in console con i privilegi di sistema consentito solo a un numero limitato di persone con accesso fisico alle sale macchine (o alla rete di OutOfBandManagement);
- accesso a sistemi informativi esterni sempre tracciato;
- piena osservanza delle prescrizioni di legge in materia di trattamento di dati personali e sensibili, con particolare riferimento agli incarichi di trattamento, e alla tenuta degli elenchi degli incaricati e dei responsabili di sistema o database;
- tracciamento e conservazione sicura dei file di log degli amministratori di sistema, data base e software complessi che accedono a sistemi con dati personali o sensibili ai sensi del D.Lgs. 196/2003.

#### 5.7. Principali procedure da implementare

Le misure minime richieste sono di seguito presentate, con *l'obiettivo di renderle operative, senza indugio, man mano che lo sviluppo dell'infrastruttura informatica della Fondazione andrà realizzandosi.*

##### 5.7.1. Copia di backup dei dati a frequenze prestabilite

Al fine di prevenire la perdita dei dati o l'interruzione dei servizi, tutti i server utilizzati per le attività comprese nel campo di applicazione del presente documento saranno sottoposti a salvataggio dei dati con cadenza giornaliera.

Per i dati maggiormente critici saranno adottate misure di "Data Disaster Recovery" che prevedano la replica remota dei dati presso una differente area geografica.

##### 5.7.2. Istituzione di password o di codici di valutazione per l'accesso ad ogni terminale

Il principio informatore della politica di gestione dei privilegi della Fondazione è che la loro assegnazione sia operata sulla base del reale bisogno di utilizzo (principio di necessità del trattamento); le autorizzazioni di accesso alle risorse devono, quindi, essere limitate ai soli dati la cui conoscenza sia necessaria e sufficiente per lo svolgimento delle operazioni di trattamento o di manutenzione affidate ad ogni persona.

Le password e i codici di valutazione per l'accesso ad ogni terminale devono essere conosciute esclusivamente dal personale preposto e modificate secondo scadenze prestabilite.

#### 5.7.3. Protezione fisica degli uffici e dei terminali

In linea generale, le sale macchine devono essere sottoposte al controllo degli accessi tramite badge individuale, singolarmente autorizzato dal Direttore, restando gli accessi registrati su opportuni file di log.

Gli accessi agli uffici devono essere controllati e regolamentati dalle procedure di accettazione della portineria, con la zona uffici protetta da varchi controllati da badge elettronici distribuiti individualmente ai dipendenti e collaboratori stabili o assegnati temporaneamente a visitatori occasionali dalla portineria, previa registrazione dell'attribuzione. I singoli piani ed uffici non saranno direttamente presidiati se non per la presenza di alcune telecamere a circuito chiuso sorvegliate dal personale di portineria. La portineria dovrà essere adeguatamente presidiata da personale dedicato, dipendente degli enti stabilmente presenti nell'edificio ovvero di ditte specializzate, secondo specifici accordi in tal senso.

E' prevista l'adozione di funzioni di screen-lock per proteggere l'accesso alla propria PdiL anche in caso di assenza temporanea.

#### 5.7.4. Identificazione di ogni responsabile all'accesso e registrazione degli accessi a dati sensibili

L'individuazione degli incaricati al trattamento dei dati personali e sensibili, degli Amministratori di Sistema e di Data Base e la registrazione dei relativi accessi deve essere conforme alle vigenti disposizioni in materia di Privacy. L'utilizzo di codici di accesso individuali, i log di sistema e le registrazioni degli accessi via rete devono consentire una adeguata registrazione degli accessi ai dati sensibili.

#### 5.7.5. Utilizzo delle postazioni di lavoro, posta elettronica aziendale e rete Internet

Per la definizione degli utilizzi consentiti delle PdiL e dei controlli che il datore di lavoro è legittimato ad effettuare, a garanzia del corretto funzionamento del sistema informativo aziendale, si rimanda alla specifica procedura da adottare con le regole comportamentali che tutti gli assegnatari di un pc (laptop e desktop) aziendale devono seguire. In particolare, tale procedura:

- evidenzia il fatto che ogni Postazione è uno strumento di lavoro che la Fondazione assegna unicamente per lo svolgimento delle attività lavorative oggetto del rapporto di lavoro;
- ribadisce il fatto che l'uso della Postazione deve sempre avvenire nel rispetto delle norme vigenti;
- conferma che la sua violazione può comportare l'applicazione delle sanzioni disciplinari previste dal vigente CCNL applicato dalla Fondazione, rimanendo ferma ogni ulteriore forma di responsabilità penale;
- definisce regole atte a prevenire infezioni da virus e codice malevolo; infatti, se la propria PdiL dovesse essere infettata, si potrebbe divenire portatori e diffusori

involontari di virus informatici su tutta la rete aziendale ma anche all'esterno grazie alla rete Internet;

- definisce regole nell'utilizzo della posta elettronica aziendale, ribadendo il fatto che non si tratta di corrispondenza personale ma di posta aziendale di pertinenza del datore di lavoro;
- definisce le regole da rispettare nella navigazione in Internet al fine di prevenire incidenti di sicurezza o di incorrere in illeciti, anche di natura penale, causati da un utilizzo indiscriminato ed inconsapevole della rete Internet;
- definisce alcune regole generali nell'utilizzo delle PdiL e nella scelta e gestione della password di accesso, al fine di evitare che terzi accedano abusivamente alle medesime;
- puntualizza che il personale deve essere consapevole delle modalità di protezione dei documenti salvati nel file server di dominio, al fine di evitare accessi non autorizzati a documenti riservati.

#### 5.7.6. Idonea formazione del personale

Idonee iniziative di formazione del personale in materia di sicurezza del trattamento dei dati sono periodicamente assunte, anche attraverso l'utilizzo di piattaforme di e-learning.

## 6. REATI IN MATERIA DI TUTELA DELLA SALUTE E SICUREZZA SUL LAVORO

Con riferimento al complesso delle disposizioni contenute nel Testo Unico sulla Salute e Sicurezza sul Lavoro (D.Lgs. 9 aprile 2008, n. 81, coordinato con il D.Lgs. 3 agosto 2009, n. 106), si provvede qui di seguito a fornire una breve descrizione dei reati che possono essere commessi in violazione delle norme sulla tutela della salute e sicurezza sul lavoro indicati all'art. 25-septies del Decreto.

Al fine di garantire l'adozione di un valido presidio contro la potenziale commissione dei suddetti reati – fermo restando il rispetto dei requisiti e l'adempimento degli obblighi previsti dalla normativa vigente – è di seguito delineato anche un sistema di gestione a tutela della salute e sicurezza dei Lavoratori, volontariamente adottato - *man mano che la struttura operativa della Fondazione andrà sviluppandosi negli uffici del Tecnopolo di Bologna* - individuando gli adempimenti essenziali affinché:

- venga predisposta un'adeguata politica aziendale,
- vengano pianificati obiettivi specifici per il perseguimento della suddetta politica,
- siano intraprese azioni, migliorative e correttive, per garantire la costante conformità al sistema di gestione adottato in tema di salute e sicurezza dei Lavoratori.

### 6.1. Le tipologie dei reati di omicidio colposo e lesioni gravi o gravissime, commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro

Le fattispecie delittuose inserite all'art. 25-septies del Decreto riguardano le ipotesi in cui l'evento sia stato determinato non già da colpa di tipo generico (imperizia, imprudenza o negligenza) bensì da *colpa specifica* che richiede che l'evento si verifichi a causa della inosservanza delle norme sulla tutela della salute e sicurezza sul lavoro; in particolare:

- il reato di *Omicidio colposo* (art. 589 cod. pen.) si configura ogni qualvolta un soggetto, in violazione delle norme per la prevenzione degli infortuni sul lavoro, cagioni, per colpa, la morte di altro soggetto;
- il reato di *Lesioni personali colpose gravi o gravissime* (art. 590 comma 3 cod. pen.) si configura ogni qualvolta un soggetto, in violazione delle norme per la prevenzione degli infortuni sul lavoro, cagioni, per colpa, ad altro soggetto lesioni gravi o gravissime; ai sensi dell'art. 583 cod. pen.,
  - la lesione è considerata *grave* se dal fatto deriva una malattia che metta in pericolo la vita della persona offesa, ovvero una malattia o un'incapacità di attendere alle ordinarie occupazioni per un tempo superiore ai quaranta giorni, e se il fatto produce l'indebolimento permanente di un senso o di un organo;
  - la lesione è considerata *gravissima* se dal fatto deriva una malattia certamente o probabilmente insanabile, la perdita di un senso, la perdita di un arto, o una mutilazione che renda l'arto inservibile, ovvero la perdita dell'uso di un organo o della capacità di procreare, ovvero una permanente e grave difficoltà del linguaggio, la deformazione, ovvero lo sfregio permanente del viso.

Perché si venga a configurare la responsabilità amministrativa della Fondazione, l'art. 5 del Decreto esige che i reati siano stati commessi dal suo personale, nel suo interesse o a suo vantaggio (ad esempio, in termini di risparmi di costi per la salute e sicurezza sul lavoro).

Per entrambe le fattispecie sopra indicate gli Enti sono soggetti a:

- una sanzione pecuniaria tra 250 e 1000 quote (il valore di ogni quota è determinato, sulla base delle condizioni economiche e patrimoniali dell'Ente, tra un minimo di euro 258 e un massimo di euro 1.549);
- una sanzione interdittiva per una durata non inferiore a tre mesi e non superiore ad un anno, consistente nelle diverse tipologie: interdizione dall'esercizio dell'attività, sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito, divieto di contrattare con la pubblica amministrazione, esclusione da agevolazioni, finanziamenti, contributi o sussidi ed eventuale revoca di quelli già concessi, divieto di pubblicizzare beni o servizi.

## 6.2. Potenziali Aree di attività a Rischio

In relazione ai reati e alle condotte criminose previste dall'art. 25 septies del Decreto, le aree ritenute più specificamente a rischio risultano essere i settori di attività dove possono concretamente essere sviluppati i fattori di rischio generali - validi per tutti i propri dipendenti ed i terzi - da individuare analiticamente nel Documento di Valutazione dei Rischi.

Il Consiglio di Amministrazione e il Direttore - anche con la collaborazione del Responsabile del Servizio di Prevenzione e Protezione (RSPP), quando identificato, e del Medico Competente, nonché su proposta dell'OdiV e del Rappresentante dei lavoratori - potranno suggerire eventuali integrazioni delle Aree di Attività a Rischio.

Con riguardo all'inosservanza delle norme poste a tutela della salute e sicurezza dei lavoratori, da cui possa discendere l'evento dannoso nelle Aree a Rischio individuate, si ritengono particolarmente sensibili le seguenti attività:

- a. determinazione della politica di salute e sicurezza sul lavoro volta a definire gli impegni generali assunti dalla Fondazione per la prevenzione dei rischi ed il miglioramento progressivo della salute e sicurezza;
- b. identificazione e corretta applicazione delle prescrizioni delle leggi e dei regolamenti applicabili in tema di sicurezza sul lavoro;
- c. identificazione e valutazione dei rischi per tutte le categorie di Lavoratori, con particolare riferimento a:
  - stesura del Documento di Valutazione dei Rischi;
  - contratti di appalto;
  - valutazione dei rischi da interferenze, ove applicabile (rif. DUVRI);
  - Piani di Sicurezza e Coordinamento, ove applicabili;
- d. determinazione di obiettivi allineati con gli impegni generali definiti nella politica di cui al punto a) ed elaborazione di programmi per il raggiungimento

di tali obiettivi con relativa definizione di priorità, tempi ed attribuzione delle rispettive responsabilità - con assegnazione delle necessarie risorse - in materia di salute e sicurezza sul lavoro, con particolare riferimento a:

- attribuzioni di compiti e doveri;
  - attività del Servizio Prevenzione e Protezione e del Medico Competente;
  - attività di tutti gli altri soggetti su cui ricade la responsabilità dell'attuazione delle misure per la salute e sicurezza dei Lavoratori;
- e. sensibilizzazione della struttura funzionale, a tutti i livelli, al fine di garantire il raggiungimento degli obiettivi prefissati, anche attraverso la programmazione di piani di formazione con particolare riferimento a:
- monitoraggio, periodicità, fruizione e apprendimento;
  - formazione differenziata per soggetti esposti a rischi specifici;
  - attuazione di adeguate attività di monitoraggio, verifica e ispezione al fine di assicurare l'efficacia del suddetto sistema di gestione della salute e sicurezza sul lavoro, in particolare per ciò che concerne:
    - misure di mantenimento e miglioramento;
    - gestione, rettifica ed inibizione dei comportamenti posti in violazione delle norme, relativi a provvedimenti disciplinari;
    - coerenza tra attività svolta e competenze possedute;
- f. attuazione delle necessarie azioni correttive e preventive in funzione del monitoraggio;
- g. effettuazione di un periodico riesame da parte della Direttore al fine di valutare l'efficacia e l'efficienza del sistema di gestione per la sicurezza del lavoro e la tutela della salute nel raggiungere gli obiettivi prefissati, nonché l'adeguatezza di questi ultimi rispetto sia alla specifica realtà della Fondazione che ad eventuali cambiamenti nell'attività.

### 6.3. Principi di comportamento

Di seguito sono riepilogati i comportamenti cui devono uniformarsi le varie funzioni aziendali, i fornitori, nonché la direzione aziendale, i Preposti e i Lavoratori, affinché non pongano in essere, non promuovano, non collaborino, o non diano causa a comportamenti tali da integrare fattispecie di reati commessi in violazione delle norme sulla tutela della salute e sicurezza dei lavoratori. In particolare, qui si intende:

- fornire un elenco dei principi generali nonché dei principi procedurali specifici cui i destinatari sono tenuti ad attenersi per una corretta applicazione del modello;
- fornire all'OdiV ed ai responsabili delle funzioni aziendali chiamati a cooperare con lo stesso, i principi e gli strumenti operativi necessari al fine di poter esercitare le attività di controllo, monitoraggio e verifica allo stesso demandati.

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole di cui al presente modello, le funzioni aziendali sono tenute, in generale, a rispettare tutte le regole e i principi contenuti nei seguenti documenti, per le parti di proprio interesse:

- Organigramma aziendale;

- Documento di Valutazione dei Rischi;
- linee guida e attività di verifica degli aggiornamenti normativi in materia antinfortunistica e di igiene e salute sul lavoro;
- linee guida sul monitoraggio dell'effettiva attuazione del sistema dei presidi descritto nel Documento di Valutazione dei Rischi, nonché sulle opportune azioni correttive e preventive ove siano evidenziate situazioni di non conformità;
- sistema disciplinare di cui al CCNL di riferimento;
- procedure ed istruzioni operative proprie del Sistema di Gestione Salute e Sicurezza sul Lavoro, o che possano avere riflessi anche indiretti sul medesimo, progressivamente adottate dalla Fondazione;
- Codice etico.

L'adozione del Modello e del Codice etico da parte della Fondazione deve essere resa nota agli appaltatori, fornitori, progettisti, fabbricanti e installatori, richiedendone conoscenza e rispetto quale obbligo contrattuale a carico di tali soggetti.

#### 6.4. Principi procedurali specifici

La Fondazione si impegna a perseguire le migliori condizioni possibili di Sicurezza e Salute del Lavoro (SSL) con riferimento alla prevenzione e al miglioramento continuo in maniera adeguata alla natura e all'entità dei rischi. La responsabilità nella gestione della SSL riguarda l'intera organizzazione, dal Datore di Lavoro sino ad ogni lavoratore; ciascuno è chiamato a dare il proprio contributo attivo, secondo le proprie attribuzioni e competenze, per concorrere agli impegni assunti dalla Direzione e per conseguire gli obiettivi concordati, utilizzando al meglio gli strumenti messi a disposizione.

Preliminarmente alla definizione degli obiettivi specifici, la Fondazione identifica i requisiti richiesti da leggi e regolamenti comunitari, nazionali, regionali e locali, anche al fine di garantire una corretta predisposizione ed implementazione del Sistema di Gestione della Salute e Sicurezza dei Lavoratori. Pertanto, il Datore di Lavoro, il suo Delegato, ma soprattutto il RSPP, al fine di armonizzare i comportamenti nell'ambito di propria competenza:

- analizzano ogni aspetto della salute e sicurezza disciplinato dal legislatore, utilizzando eventuali banche dati esistenti, documenti di associazioni imprenditoriali, sindacali, etc.;
- individuano le disposizioni normative che interessano la Fondazione, sulla base dell'attività svolta;
- procedono all'individuazione dei requisiti e degli adempimenti derivanti dal rispetto di tali norme applicabili all'attività svolta dalla Fondazione.

Nella gestione delle attività della Fondazione, si assumono i seguenti *Impegni*:

- considerare la prevenzione di infortuni e malattie e il miglioramento costante della gestione SSL e dei relativi risultati - avendo come costante riferimento le "misure generali di tutela" stabilite dal Decreto 81/2008 e ss.mm.ii. - come parte integrante della gestione aziendale;

- assicurare il rispetto, nella sostanza e nello spirito informatore, delle leggi e dei regolamenti di SSL applicabili - a cominciare, appunto, dal decreto 81/2008 - nonché degli impegni derivanti dai contratti di lavoro e dagli altri liberamente assunti, tenuto conto dell'attività svolta e della dimensione aziendale;
- assicurare il coinvolgimento e la consultazione dei lavoratori per riesaminare periodicamente la politica stessa e il sistema di gestione attuato, definendone e diffondendone all'interno dell'azienda gli obiettivi di SSL e i relativi programmi di attuazione;
- assicurare il riesame periodico dei risultati ottenuti con il sistema di gestione - da condurre anche durante la riunione periodica di prevenzione e protezione con il Medico Competente, il RSPP e i rappresentanti dei lavoratori per la sicurezza - sulla base di una relazione strutturata per riassumere i dati dei monitoraggi e della sorveglianza svolti sul sistema, sui processi e sul personale.

Per tradurre nella pratica operativa gli impegni di cui sopra, si intendono perseguire i seguenti *Obiettivi* generali:

- identificare e monitorare le leggi, i regolamenti e le regole tecniche, relativi alla SSL, applicabili alla nostra organizzazione, per tradurre i requisiti in compiti e disposizioni interne e così operare nel rispetto della normativa di salute e sicurezza applicabile;
- perseguire i miglioramenti possibili nelle direzioni delineate dagli orientamenti nazionali e internazionali, pubblicati in norme tecniche, linee guida, codici di buone pratiche e simili;
- promuovere attività di sensibilizzazione e formazione sulla gestione della sicurezza dei propri dipendenti, collaboratori, fornitori e appaltatori;
- valutare in anticipo i nuovi ambienti, impianti, processi, tecnologie, attività, prodotti e servizi approvvigionati, per identificarne i pericoli e valutarne i rischi per la SSL, così da assicurarne il controllo, anche ai fini del miglioramento delle prestazioni;
- adottare le migliori tecniche e procedure di prevenzione e controllo delle emergenze;
- assicurare il coinvolgimento delle funzioni direttive nello sviluppo della politica, degli impegni e degli obiettivi di SSL; assicurare che tutto il personale sia responsabilizzato negli impegni di SSL, sia coinvolto nel perseguirli, sia istruito e formato a adottare i comportamenti coerenti con tali impegni; garantire il coinvolgimento nel sistema, per quanto applicabile, di progettisti, fabbricanti, fornitori, installatori, nonché di appaltatori e prestatori d'opera;
- consultare regolarmente i rappresentanti dei lavoratori per la sicurezza; monitorare e valutare in maniera appropriata le prestazioni (i risultati) del sistema di gestione SSL per stabilirne l'adeguatezza e l'efficacia e perseguirne il miglioramento continuo;
- riesaminare periodicamente la politica SSL per assicurare che gli impegni, gli obiettivi, le risorse e gli strumenti siano significativi e appropriati per la nostra realtà organizzativa;
- promuovere e mantenere un atteggiamento aperto, costruttivo, trasparente nei confronti del pubblico, degli utenti, delle autorità pubbliche e delle altre parti interessate.

Quanto sopra è comunicato a tutte le persone che operano nell'ambito dell'organizzazione, perché ne siano consapevoli e motivate ad applicarla, per quanto di loro competenza e nella loro possibilità; la documentazione prodotta resta disponibile alle parti interessate e a chiunque ne faccia motivata richiesta.

#### 6.5. Processo di pianificazione e definizione dell'organizzazione

Al fine di dare attuazione alla politica di cui al precedente paragrafo, la Fondazione:

- definisce gli obiettivi finalizzati al mantenimento e miglioramento del Sistema di Gestione SSL;
- predispone un piano per il raggiungimento di ciascun obiettivo, l'individuazione delle figure/strutture coinvolte nella realizzazione del suddetto piano e l'attribuzione dei relativi compiti e responsabilità;
- definisce le risorse, anche economiche, necessarie;
- prevede le modalità di verifica dell'effettivo ed efficace raggiungimento degli obiettivi.

Nella definizione dei compiti organizzativi ed operativi interni devono, inoltre, essere documentate e rese note a tutti i livelli dell'organizzazione le funzioni e i compiti del Datore di Lavoro e dei suoi delegati, dei Preposti, del Responsabile del Servizio di Prevenzione e Protezione e degli Addetti, dei Rappresentanti dei Lavoratori per la Sicurezza e degli addetti alla gestione delle emergenze, nonché i compiti e le responsabilità del Medico Competente.

#### 6.6. Informazione, formazione ed addestramento

L'informazione che la Fondazione destina alle varie funzioni aziendali deve essere facilmente comprensibile e deve consentire agli stessi di acquisire la necessaria consapevolezza in merito a:

- le conseguenze derivanti dallo svolgimento della propria attività non conformemente al Sistema di Gestione SSL adottato dalla Fondazione;
- il ruolo e le responsabilità che ricadono su ciascuno di esso e l'importanza di agire in conformità con la politica aziendale e le procedure definite, nonché con i principi indicati in questo capitolo.

A tale scopo, la Fondazione, in considerazione dei diversi ruoli, responsabilità e capacità e dei rischi cui è esposta ciascuna funzione aziendale, fornisce, tra l'altro, *adeguata informazione* ai lavoratori sulle seguenti tematiche:

- rischi specifici dell'impresa, sulle loro conseguenze, sulle misure di prevenzione e protezione adottate, e sulle conseguenze che il mancato rispetto di tali misure può provocare anche ai sensi del Decreto;
- procedure che riguardano il primo soccorso, la lotta antincendio, l'evacuazione dei luoghi di lavoro;
- Servizio di Prevenzione e Protezione: nominativi del RSPP e del Medico Competente.

Fornisce, inoltre, *adeguata formazione* a tutti i lavoratori in materia di sicurezza sul lavoro, i cui contenuti, secondo le previsioni del Decreto, siano facilmente comprensibili e consentano di acquisire le conoscenze e competenze necessarie. A tal proposito, si specifica che:

- il RSPP provvede alla stesura del piano di formazione condividendolo con il Medico Competente;
- ulteriori attività integrative a tale piano dovranno essere attuate in presenza di innovazioni tecnologiche, nuove attrezzature o necessità di introdurre nuove procedure di lavoro;
- la formazione deve essere adeguata ai rischi della mansione cui ognuno dei Lavoratori è in concreto assegnato e deve prevedere questionari di valutazione dell'apprendimento;
- ognuno dei lavoratori deve essere sottoposto a tutte quelle azioni formative rese obbligatorie dalle normative di legge quali, ad esempio:
  - uso delle attrezzature di lavoro e dei dispositivi di protezione individuale;
  - movimentazione manuale di carichi;
  - uso dei videoterminali;
  - segnaletica visuale, gestuale, vocale, luminosa e sonora e ogni altro argomento che, di volta in volta, venga considerato necessario per il raggiungimento degli obiettivi aziendali in tema di SSL;
- i lavoratori che eventualmente cambiano mansione e quelli “distaccati” devono fruire di formazione specifica, preventiva o aggiuntiva, ove necessario, per il nuovo incarico;
- gli addetti a specifici compiti in materia di emergenza (es. addetti alla prevenzione incendi ed evacuazione e pronto soccorso) devono ricevere specifica formazione;
- sia il Delegato del Datore di Lavoro che il Preposto ricevono, a cura del Datore di Lavoro, un'adeguata e specifica formazione e un aggiornamento periodico in relazione ai propri compiti in materia di SSL; i contenuti di tale formazione comprendono:
  - principali soggetti coinvolti e i relativi obblighi;
  - definizione e individuazione dei fattori di rischio;
  - valutazione dei rischi;
  - individuazione delle misure tecniche, organizzative e procedurali di prevenzione e protezione.
- devono essere effettuate periodiche esercitazioni di emergenza di cui deve essere data evidenza (attraverso, ad esempio, la verbalizzazione dell'avvenuta esercitazione con riferimento alle modalità di svolgimento e alle risultanze);
- i neoassunti – in assenza di pregressa esperienza professionale/lavorativa e di adeguata qualificazione – non possono essere adibiti in autonomia ad attività operativa ritenuta più a rischio infortuni se non dopo l'acquisizione di un grado di professionalità idoneo allo svolgimento della stessa mediante adeguata formazione.

Di tutta l'attività di formazione sopra descritta deve essere data evidenza su base documentale, anche mediante apposita verbalizzazione, e laddove previsto, deve essere ripetuta periodicamente.

## 6.7. Comunicazione, partecipazione e consultazione

Al fine di dare maggior efficacia al sistema organizzativo adottato per la gestione della sicurezza e quindi alla prevenzione degli infortuni sul luogo di lavoro, la Fondazione si organizza per garantire un adeguato livello di circolazione e condivisione delle informazioni tra tutti i Lavoratori e verso l'esterno.

### 6.7.1. Comunicazione interna

La Fondazione adotta un sistema di comunicazione interna che prevede due differenti tipologie di flussi informativi:

- *dal basso verso l'alto*, mettendo a disposizione apposite schede di segnalazione attraverso la compilazione delle quali ciascuno dei Lavoratori ha la possibilità di portare a conoscenza del proprio superiore gerarchico e del SPP, osservazioni, proposte ed esigenze di miglioria inerenti alla gestione della sicurezza in ambito aziendale;
- *dall'alto verso il basso*, diffondendo a tutti i Lavoratori la conoscenza del sistema adottato per la gestione della sicurezza nel luogo di lavoro.

A tale scopo, la Fondazione garantisce alle funzioni operative un'adeguata e costante informativa attraverso la predisposizione di comunicati da diffondere internamente e l'organizzazione di incontri periodici che abbiano ad oggetto:

- nuovi rischi in materia di salute e sicurezza dei Lavoratori;
- modifiche nella struttura organizzativa adottata per la gestione della salute e sicurezza dei Lavoratori;
- contenuti delle procedure aziendali adottate per la gestione della sicurezza e salute dei Lavoratori;
- ogni altro aspetto inerente alla salute e alla sicurezza dei Lavoratori.

### 6.7.2. Comunicazione esterna

La Fondazione si attiva per rendere edotte le persone esterne in visita (ad es.: appaltatori, fornitori, clienti, visitatori) sugli eventuali rischi collegati alla loro presenza in sede, mediante:

- informazione diretta;
- segnaletica di sicurezza e specifica cartellonistica presente negli ambienti di lavoro;
- planimetrie che illustrano le modalità di evacuazione in caso di pericolo grave ed immediato, esposte negli ambienti;
- consegna di apposito opuscolo informativo.

È prevista una apposita procedura che regoli il coordinamento e la cooperazione tra datori di lavoro, per i lavori in appalto o contratto d'opera, da realizzarsi da parte di aziende terze (fornitori) all'interno degli ambienti di lavoro della Fondazione.

Altre forme di comunicazione esterna messa in atto dalla Fondazione riguardano:

- la richiesta di soccorsi esterni in caso di emergenza, per le quali si utilizzano le modalità individuate nel Piano di Emergenza Interno;
- la comunicazione agli organi di controllo competenti per territorio della designazione del RSPP.

### 6.7.3. Gestione della documentazione

La documentazione del Sistema di gestione SSL costituisce la struttura intorno alla quale esso si articola, lo descrive e definisce le azioni da intraprendere, le modalità di attuazione, chi deve fare che cosa, quali registrazioni devono essere mantenute. È importante che la documentazione sia mantenuta ad un livello minimo necessario ai fini dell'efficacia ed efficienza del sistema; essa deve, infatti, essere un ausilio all'applicazione del sistema e non un inutile dispendio di tempo e di risorse.

La Fondazione:

- predispone un sistema documentale snello, atto a consentire a tutto il personale la facile e rapida consultazione di ogni documentazione connessa;
- pianifica le modalità per l'aggiornamento, in tempo utile ai bisogni, e la conservazione della propria documentazione;
- cura la sua realizzazione concreta;
- affida al RSPP la responsabilità della gestione documentale e definisce modalità per:
  - stabilire i contenuti e il formato dei documenti (supporti elettronici, cartacei, audiovisivi);
  - definire il collegamento tra la documentazione e il flusso informativo in modo da assicurare l'accurata distribuzione della documentazione a tutto e al solo personale interessato;
  - rimuovere tutti i documenti superati dai luoghi di utilizzo e archiviare adeguatamente quelli utili a fini legali o come memoria storica;
  - definire le necessità di rinnovo e archiviazione dei documenti e le relative modalità, fissando, in particolare, i tempi di archiviazione;
  - documentare e registrare le attività di consultazione, coinvolgimento, informazione e formazione del personale.

### 6.8. Monitoraggio e riesame

L'attività di verifica del Sistema di gestione SSL mira a valutarne l'effettiva attuazione; essa prevede una fase di verifica del raggiungimento degli obiettivi ed una fase di verifica della funzionalità del sistema stesso. È uno dei motori del miglioramento continuo, visto che, attraverso le verifiche, si vogliono valutare le prestazioni del sistema, rispetto a quanto pianificato, e fornire alla Direzione informazioni importanti sulla sua adeguatezza per conseguire i risultati attesi.

In particolare, la Fondazione:

- definisce le modalità per monitorare e misurare con regolarità le principali attività gestite che possono avere ricadute sulla SSL;

- stabilisce le modalità e le responsabilità del monitoraggio in sede di pianificazione, in conformità al suo schema organizzativo e funzionale e alle relative responsabilità di gestione operativa;
- attua un programma di audit del Sistema di gestione SSL al fine di stabilire se è conforme a quanto pianificato e correttamente applicato, mantenuto attivo e consente di raggiungere gli obiettivi.

I risultati degli audit sono utilizzati alla Direzione per la definizione delle decisioni strategiche di propria competenza, durante il riesame del Sistema di gestione SSL.

Dopo la conclusione del ciclo di monitoraggio interno, il vertice aziendale deve sottoporre a riesame le attività del Sistema di gestione SSL, per valutare se sia adeguatamente attuato e si mantenga idoneo al conseguimento degli obiettivi e della politica della sicurezza stabilita. Argomenti tipici del riesame possono essere:

- statistiche infortuni e malattie professionali;
- risultati dei monitoraggi interni, compresi infortuni, incidenti e malattie professionali;
- relazioni periodiche del Medico competente;
- azioni correttive intraprese;
- rapporti sulle emergenze (reali o simulate);
- cambiamenti dell'organizzazione o della situazione al contorno (per esempio, modifiche di processi, nuovi contratti di lavoro, modifiche legislative);
- rapporti dal RSPP,
- informazioni risultanti dalle attività di consultazione del personale;
- rapporti sulla efficacia del sistema di gestione;
- rapporti sulla identificazione dei pericoli e sulla valutazione e controllo dei rischi.

Il momento del riesame della Direzione chiude il processo di gestione e nello stesso tempo lo ricomincia:

- riesaminando lo stato del sistema e i risultati della gestione SSL in un dato periodo e, di conseguenza,
- riformulando la politica e gli obiettivi per il periodo successivo, nell'ottica del miglioramento progressivo.

#### 6.9. I contratti di appalto

Nei contratti di appalto (intesi come contratto di appalto d'opera, di servizi o contratto d'opera o di somministrazione) il Datore di Lavoro, in caso di affidamento di lavori, servizi e forniture all'impresa appaltatrice o a Lavoratori autonomi all'interno delle aree di pertinenza della Fondazione – così come andranno sviluppandosi nel Tecnopolo di Bologna - è chiamato a:

- verificare l'idoneità tecnico-professionale delle imprese appaltatrici o dei Lavoratori autonomi in relazione alle attività da affidare in appalto;
- mettere a disposizione degli appaltatori informazioni dettagliate circa i rischi specifici esistenti nell'ambiente in cui sono destinati ad operare e in merito alle misure di prevenzione e di emergenza adottate in relazione alla propria attività;
- cooperare all'attuazione delle misure di prevenzione e protezione dai rischi sul lavoro incidenti sull'attività lavorativa oggetto dell'appalto;

- coordinare gli interventi di protezione e prevenzione dai rischi cui sono esposti i Lavoratori, attraverso un costante scambio di informazioni con i datori di lavoro delle imprese appaltatrici anche al fine di eliminare i rischi dovuti alle interferenze tra i lavori delle diverse imprese coinvolte nell'esecuzione dell'opera complessiva.

Il Datore di Lavoro committente promuove la cooperazione ed il coordinamento di cui ai punti precedenti elaborando un Documento Unico di Valutazione dei Rischi per le Interferenze (DUVRI) nel quale siano indicate le misure adottate per eliminare o, laddove non sia possibile, per ridurre al minimo i rischi da interferenze. Tale documento deve allegarsi al contratto di appalto o d'opera, già in fase di procedura di affidamento, e va adeguato in funzione dell'evoluzione dei lavori, dei servizi e delle forniture. L'obbligo di redazione del suddetto documento non sussiste in caso di appalto di servizi di natura intellettuale, mere forniture di materiali o attrezzature nonché per i lavori o servizi la cui durata non sia superiore ai due giorni, sempre che essi non comportino rischi derivanti dalla presenza di agenti cancerogeni, biologici, atmosfere esplosive o rischi particolari così come individuati nell'allegato XI del D.Lgs. 81/08.

Nei contratti di somministrazione (art. 1559 c.c.), di appalto (art. 1655 c.c.) e di subappalto (art. 1656 c.c.), devono essere specificamente indicati i costi delle misure adottate per eliminare o, ove ciò non sia possibile, ridurre al minimo i rischi in materia di salute e sicurezza sul lavoro, derivanti dalle interferenze delle lavorazioni; tali costi non sono soggetti a ribasso. Relativamente agli appalti soggetti alla normativa di cui al Codice Appalti, la Fondazione osserverà, tra l'altro, i seguenti adempimenti:

- non sono ammessi a negoziare operatori economici che hanno commesso gravi infrazioni, debitamente accertate alle norme in materia di sicurezza, e a ogni altro obbligo derivante dai rapporti di lavoro, risultanti dai dati in possesso dell'Osservatorio;
- nella predisposizione delle gare di appalto e nella valutazione dell'anomalia delle offerte nelle procedure di affidamento di appalti di lavori pubblici, di servizi e di forniture, la Fondazione è tenuta a valutare che il valore economico sia adeguato e sufficiente rispetto al costo del lavoro e al costo relativo alla sicurezza, il quale deve essere specificamente indicato e risultare congruo rispetto all'entità e alle caratteristiche dei lavori, dei servizi o delle forniture.

Nei contratti con gli appaltatori, Fornitori, Progettisti, Fabbricanti e Installatori deve essere contenuta apposita clausola che richiami il rispetto del Modello e del Codice Etico.

#### 6.10. Applicazione del modello e OdiV

Il Datore di Lavoro individua il Responsabile interno dell'effettiva attuazione dei principi comportamentali sopra segnalati che può corrispondere alla funzione del Direttore, in quanto Datore di Lavoro ai fini della normativa di SSL, o suoi Delegati in materia di SSL.

Il Responsabile interno dovrà:

- mettere a disposizione dell'OdiV la documentazione per eventuali verifiche dirette;
- inviare all'OdiV un report informativo, con cadenza semestrale, una volta approvato il Modello, sugli episodi eventualmente occorsi, sulle attività di controllo effettuate e sullo stato di attuazione delle previsioni in materia di SSL.

I compiti di vigilanza dell'OdiV in relazione all'osservanza del Modello per quanto concerne i Reati di cui all'art. 25 septies del Decreto sono i seguenti:

- proporre eventuali aggiornamenti delle istruzioni relative ai comportamenti da seguire nell'ambito delle Aree a Rischio;
- svolgere verifiche periodiche, anche a sorpresa, sul rispetto delle procedure interne;
- esaminare eventuali segnalazioni specifiche ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute;
- proporre al Consiglio di Amministrazione le eventuali integrazioni alle procedure esistenti per rendere più efficaci le azioni di prevenzione e repressione delle condotte vietate.

## 7. REATI SOCIETARI

### 7.1. Quadro di riferimento

Questa parte è relativa ai reati societari compiuti nell'interesse della Fondazione da soggetti specificamente individuati dalla norma, quali amministratori, dirigenti e dipendenti operanti nelle aree di attività a rischio, nonché da collaboratori esterni; essa ha lo scopo di:

- individuare ed illustrare le fattispecie di reati societari per i quali, in caso di commissione da parte di soggetti con interesse per la Fondazione, è prevista la responsabilità amministrativa in capo alla medesima;
- indicare le “regole di comportamento” e le procedure che gli amministratori, i dirigenti ed i dipendenti, nonché i collaboratori esterni, sono chiamati ad osservare ai fini della corretta applicazione del Modello;
- fornire all'OdiV ed ai responsabili delle funzioni gli elementi di riferimento per l'esercizio delle attività di controllo, monitoraggio e verifica.

Nel corso della gestione sociale, oltre alle regole di cui al presente Modello, i soggetti coinvolti devono in generale conoscere e rispettare, con riferimento alle mansioni effettivamente espletate, le regole ed i principi contenuti nei seguenti documenti:

- Statuto;
- Codice Etico;
- Regolamento per la disciplina dei conflitti d'interesse;
- Istruzioni operative per la redazione dei bilanci e dei documenti collegati;
- Principi contabili di riferimento e Piano dei conti di contabilità generale;
- ogni altra normativa interna relativa al sistema di controllo in essere nella Fondazione.

### 7.2. Reati societari identificati dal Decreto

L'art. 25-ter del Decreto definisce puntualmente le sanzioni pecuniarie derivanti da reati in materia societaria previsti dal codice civile, se commessi nell'interesse della società, da amministratori, direttori generali o liquidatori o da persone sottoposte alla loro vigilanza, qualora il fatto non si fosse realizzato se essi avessero vigilato in conformità degli obblighi inerenti alla loro carica; in particolare, le sanzioni sono quantificate specificamente per i seguenti delitti e contravvenzioni:

- a) false comunicazioni sociali (art. 2621 cod. civ.);
- b) false comunicazioni sociali in danno dei soci o dei creditori (art. 2622, primo e terzo comma, cod. civ.);
- c) impedito controllo (art. 2625, secondo comma, cod. civ.);
- d) formazione fittizia del capitale (art. 2632 cod. civ.);
- e) indebita restituzione dei conferimenti (art. 2626 cod. civ.);
- f) illegale ripartizione degli utili e delle riserve (art. 2627 cod. civ.);
- g) illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 cod. civ.);
- h) operazioni in pregiudizio dei creditori (art. 2629 cod. civ.);

- i) indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 cod. civ.);
- j) illecita influenza sull'assemblea (art. 2636 cod. civ.);
- k) aggio (art. 2637 cod. civ.);
- l) omessa comunicazione del conflitto d'interessi (art. 2629-bis cod. civ.);
- m) ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638, primo e secondo comma, cod. civ.).

Se, in seguito alla commissione dei reati suddetti, l'ente ha conseguito un profitto di rilevante entità, la sanzione pecuniaria è aumentata di un terzo.

### 7.3. I processi sensibili

Nell'ambito delle attività svolte dalla Fondazione i processi sensibili che risultano attinenti con i reati societari sono individuati nei seguenti:

- predisposizione delle comunicazioni a Membri fondatori, Partner e terzi, relative alla situazione economica, patrimoniale e finanziaria della Fondazione, tipicamente il bilancio di esercizio;
- gestione dei rapporti con il Collegio dei Sindaci e con la Società di Revisione, in quanto soggetti che svolgono le attività di controllo dei conti e delle risultanze di gestione;
- tenuta della contabilità e gestione degli adempimenti fiscali e previdenziali.

Tali processi devono risultare adeguatamente formalizzati e dovranno essere periodicamente sottoposti a monitoraggio da parte dell'OdiV.

In relazione alle attività potenzialmente a rischio di reato, i soggetti indicati svolgono i seguenti compiti:

- gli Studi di Commercialisti, Consulenti fiscali/tributari e Consulenti del Lavoro, allo scopo incaricati, si occupano di inserire le rilevazioni contabili durante l'esercizio, di predisporre i cedolini mensili degli stipendi, di predisporre la bozza del bilancio d'esercizio, di adempiere alle relative obbligazioni di natura fiscale e tributaria;
- il Direttore svolge attività di coordinamento con gli Studi di Commercialisti, Consulenti fiscali/tributari e Consulenti del Lavoro e finalizza la bozza del bilancio d'esercizio; si avvale di un ufficio amministrativo.

Le attività di gestione della contabilità sono disciplinate prevalentemente da riferimenti normativi, da principi contabili nazionali, da istruzioni verbali, nonché da prassi consolidate.

Tutte le movimentazioni finanziarie transitano dai conti correnti bancari ed hanno riscontro nella contabilità tenuta dallo Studio di Commercialisti, che dedica una persona con esperienza pluriennale nella tenuta della contabilità di aziende di piccole e medie dimensioni. Si evidenziano differenti livelli di controllo:

- il potere di disposizione sui conti bancari è attribuito esclusivamente al Presidente ed al Direttore, prevalentemente mediante homebanking, con l'ufficio amministrativo che predispose le disposizioni di bonifico;
- di ogni pagamento si dà evidenza scritta sulla copia cartacea del documento di addebito, trasmettendola allo Studio di Commercialisti che procede alla registrazione contabile traendo gli originali delle fatture dal cassetto fiscale della Fondazione;
- la riconciliazione fra gli estratti conto bancari e le risultanze contabili è effettuata su base corrente.
- la tenuta, conservazione e aggiornamento delle rilevazioni e delle risultanze contabili, con l'evidenza dei relativi adempimenti di pubblicità, è assicurata dallo Studio di Commercialisti allo scopo incaricato.

Il Collegio dei Sindaci viene regolarmente informato della convocazione delle assemblee e delle riunioni del Consiglio di Amministrazione e vengono loro trasmessi i documenti necessari al fine di poter effettuare le relative verifiche.

La correttezza del bilancio d'esercizio, ai fini della rappresentazione dei fatti di gestione, è assicurata dall'attività di revisione legale dei conti svolta dalla Società di Revisione, come stabilito dall'art. 17 dello Statuto; pertanto, il bilancio d'esercizio è considerato affidabile e in grado di rappresentare correttamente i fatti di gestione nell'interesse dei membri fondatori, dei creditori e dei terzi interessati ad instaurare dei rapporti con la Fondazione.

Il Consiglio di Amministrazione approva, altresì, il bilancio di previsione dell'esercizio successivo, entro il mese di novembre, in base alle risultanze contabili pre-consuntive, integrate con le opportune informazioni extracontabili, ed ai piani di sviluppo in corso e previsti.

#### 7.4. I principi generali di comportamento

I principi di comportamento di seguito elencati sono finalizzati a limitare il più possibile il verificarsi dei reati previsti nel Decreto e devono essere adottati sia dagli amministratori e dirigenti, sia da tutto il personale della Fondazione direttamente coinvolto nelle attività inerenti i potenziali reati societari, sia i collaboratori esterni che devono in generale conoscere e rispettare le norme inerenti il sistema amministrativo, contabile e finanziario della Fondazione. In particolare, si pone:

- l'espresso divieto di porre in essere comportamenti tali che, presi individualmente o collettivamente, integrino - direttamente, indirettamente o potenzialmente - le fattispecie di reato previste dall'art. 25 ter del Decreto;
- l'espresso obbligo a carico dei soggetti sopra indicati di rispettare le norme di legge e le procedure interne in tutte le attività connesse alla formazione del bilancio e delle altre comunicazioni sociali tenendo un comportamento corretto, trasparente e collaborativo; con riferimento al comportamento richiesto, è vietata:
  - la rappresentazione o trasmissione di dati falsi, lacunosi o, comunque, non rispondenti alla realtà, sulla situazione economica, patrimoniale e finanziaria della Fondazione per la redazione di bilanci, relazioni e prospetti o altre comunicazioni sociali e l'informativa in genere;

- l'omissione di dati ed informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria della Fondazione.
- l'espresso obbligo di assicurare il regolare funzionamento della Fondazione e del Consiglio di Amministrazione, garantendo ed agevolando ogni forma di controllo interno sulla gestione sociale previsto dalla legge, nonché la libera e corretta formazione della volontà assembleare; nell'ambito dei suddetti comportamenti, è fatto divieto, in particolare, di:
  - porre in essere comportamenti che impediscano o, comunque, ostacolino, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, lo svolgimento dell'attività di controllo e di revisione della gestione sociale da parte dei revisori contabili e dei sindaci;
  - porre in essere, in occasione di assemblee, atti simulati o fraudolenti finalizzati ad alterare il regolare procedimento di formazione della volontà assembleare;
- l'espresso obbligo di effettuare con tempestività, correttezza e completezza tutte le comunicazioni previste dalla legge e dai regolamenti nei confronti delle Autorità pubbliche e di Vigilanza, non frapponendo alcun ostacolo all'esercizio delle funzioni da queste esercitate. In ordine a tale punto, è fatto divieto di:
  - omettere di effettuare, con la dovuta chiarezza, completezza e tempestività, nei confronti delle Autorità in questione, tutte le comunicazioni, periodiche e non, nonché la trasmissione dei dati e documenti, previsti dalla legge e dalla ulteriore normativa di settore o specificamente richiesti dalle predette Autorità;
  - esporre in tali comunicazioni e nella documentazione trasmessa fatti non rispondenti al vero oppure occultare fatti concernenti la situazione economica, patrimoniale o finanziaria della Fondazione;
  - porre in essere qualsiasi comportamento che sia di ostacolo all'esercizio delle funzioni da parte delle Autorità pubbliche e di Vigilanza, anche in sede di ispezione (es.: espressa opposizione, rifiuti pretestuosi, comportamenti ostruzionistici o di mancata collaborazione, quali ritardi nelle comunicazioni o nella messa a disposizione di documenti).

Infine, tutti coloro che siano in possesso di informazioni privilegiate, derivanti dal loro rapporto di lavoro con la Fondazione non dovranno divulgare a terzi, direttamente o indirettamente, informazioni rilevanti che non siano di dominio pubblico.

La presenza di procedure informali e prassi consolidate consente di attenuare ma non di neutralizzare i rischi connessi alla mancanza di procedure formalizzate per la rilevazione e contabilizzazione delle poste di bilancio; pertanto, si segnala l'opportunità che i flussi informativi siano progressivamente formalizzati, in corrispondenza con la crescita dimensionale dell'operatività, con il precipuo obiettivo di ridurre le ipotesi di condotta illecita di carattere doloso da parte dei soggetti che operano per la corretta rappresentazione contabile della realtà della Fondazione.

#### 7.5. I controlli dell'Organismo di Vigilanza

L'OdiV effettua periodicamente controlli a campione sulle attività connesse ai "processi sensibili" diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello; a tal fine, all'OdiV viene garantito libero accesso a tutta la documentazione aziendale rilevante così come previsto nella Parte Generale del Modello. Inoltre, l'OdiV può attivarsi con specifici controlli diretti e indiretti a seguito delle segnalazioni ricevute, secondo quanto riportato nella Parte Generale del Modello. In particolare, è compito dell'OdiV:

- a) verificare che la Fondazione emani e aggiorni le istruzioni standardizzate relative a:
  - una compilazione omogenea e coerente della documentazione inerente le operazioni a rischio seguite dai Responsabili Interni;
  - gli atteggiamenti da assumere nell'ambito delle Attività a rischio e, in particolare, nella predisposizione di comunicazioni sociali;
  - la trasmissione di dati ed informazioni alla funzione responsabile attraverso un sistema, anche informatico, che consente la tracciatura dei singoli passaggi e l'identificazione dei soggetti che inseriscono i dati nel sistema;
- b) con riferimento al bilancio, alle relazioni e alle altre comunicazioni sociali previste dalla legge - in ragione della circostanza che il bilancio della Fondazione è sottoposto a verifica della Società di Revisione - provvedere all'espletamento dei seguenti compiti:
  - monitoraggio sull'efficacia delle procedure interne per la prevenzione del reato di false comunicazioni sociali;
  - esame di eventuali segnalazioni specifiche provenienti dagli organi di controllo o da qualsiasi dipendente ed effettuazione degli accertamenti ritenuti necessari od opportuni in conseguenza delle segnalazioni ricevute;
- c) effettuare con riferimento alle altre attività a rischio:
  - verifiche periodiche sul rispetto delle procedure interne;
  - verifiche periodiche sull'effettuazione delle comunicazioni alle Autorità pubbliche e/o di Vigilanza e sull'osservanza delle procedure adottate nel corso di eventuali ispezioni compiute dai funzionari di queste ultime;
  - monitoraggio sull'efficacia delle verifiche a prevenire la commissione di reati;
  - l'esame di eventuali segnalazioni specifiche provenienti dagli organi di controllo o da qualsiasi dipendente gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.
- d) verificare il rispetto e la corretta applicazione delle prescrizioni previste nei processi sensibili da parte dei soggetti aziendali coinvolti sulla procedura e verificare periodicamente, con il supporto delle altre funzioni competenti, la validità delle procedure finalizzate:
  - all'osservanza dei Destinatari delle disposizioni del Decreto;
  - all'attuazione di meccanismi sanzionatori qualora si accertino violazioni delle prescrizioni.

## 8. REATI DI RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA

### 8.1. Quadro di riferimento

I reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, richiamati dalla disposizione di cui all'art. 25-octies del Decreto, che stabilisce le relative sanzioni in termini di responsabilità amministrativa dell'ente:

- sono identificati dagli artt. 648 c.p. (Ricettazione), 648 bis c.p. (Riciclaggio) e dell'art. 648 ter c.p. (Impiego di denaro, beni o utilità di provenienza illecita);
- possono essere compiuti da soggetti aziendali quali amministratori, dirigenti e dipendenti della Fondazione che, in ragione delle loro cariche o funzioni, curano i flussi finanziari aziendali o le procedure di approvvigionamento.

Obiettivi di questa parte del Modello sono:

- individuare ed illustrare le fattispecie di reato incluse tra i reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita per i quali, in caso di commissione da parte di soggetti aziendali con contemporaneo interesse o vantaggio per la Fondazione, è prevista la responsabilità amministrativa in capo alla Fondazione medesima;
- indicare le “regole di comportamento” e le procedure che gli amministratori, i dirigenti ed i dipendenti, nonché i collaboratori esterni, sono chiamati ad osservare ai fini della corretta applicazione del Modello per quanto inerente i suddetti reati;
- fornire all'OdiV ed ai responsabili delle funzioni aziendali gli elementi di riferimento per l'esercizio delle attività di controllo, monitoraggio e verifica.

La funzione aziendale maggiormente esposta a rischio per queste tipologie di reato è quella amministrativo-finanziario.

### 8.2. Potenziali attività a rischio

Nell'ambito delle possibili attività svolte dalla Fondazione, i processi sensibili che risultano attinenti ai reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita sono individuati nella gestione di:

- rapporti e flussi finanziari in entrata ed in uscita, intrattenuti con soggetti terzi;
- approvvigionamenti di beni e servizi;
- alienazioni di cespiti.

Tali processi devono risultare adeguatamente formalizzati e dovranno essere periodicamente sottoposti a monitoraggio da parte dell'OdiV.

Nel processo di selezione dei fornitori e dei partner commerciali devono essere osservate prassi che assicurino sufficienti garanzie in ordine al rischio che siano instaurati rapporti con controparti contrattuali/partner commerciali implicati in

vicende relative al riciclaggio di denaro proveniente da attività illecite o criminali, o relazioni che implicino ricettazione di beni.

Adeguate procedure devono assicurare la verifica dell'attendibilità commerciale e professionale dei fornitori e partner commerciali/finanziari, individuando parametri che possano aiutare ad identificare soggetti "a rischio" di rapporti con organizzazioni criminali o implicati in vicende relative al riciclaggio. Alcuni dati o informazioni utili potrebbero essere:

- nominativi degli amministratori;
- soci di riferimento e professione degli stessi; se i soci di riferimento sono a loro volta persone giuridiche, è necessario risalire nelle partecipazioni sociali fino al raggiungimento delle prime persone fisiche;
- dati pregiudizievoli pubblici, quali protesti e procedure concorsuali;
- entità del prezzo sproporzionata rispetto ai valori medi di mercato;
- coinvolgimento di "persone politicamente esposte", come definite all'art. 1 dell'Allegato tecnico del D. Lgs. 21 novembre 2007, n. 231, di attuazione della direttiva 2005/60/CE);

Per importi superiori ad Euro 50.000,00 è necessario richiedere al fornitore di produrre il certificato di iscrizione alla Camera di Commercio con dicitura antimafia.

### 8.3. Principi generali di comportamento

In occasione dell'instaurarsi di rapporti finanziari con soggetti terzi o di approvvigionamento di beni e/o servizi devono essere adottate idonee regole di condotta finalizzate a limitare il più possibile il rischio del verificarsi dei reati previsti nel Decreto; tali regole si applicano direttamente agli amministratori, dirigenti e dipendenti, nonché ai collaboratori esterni. In particolare, è fatto espresso divieto di porre in essere:

- comportamenti tali che, individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 25-octies del Decreto);
- comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo.

Nell'ambito dei suddetti comportamenti è fatto obbligo di:

- operare nel rispetto della normativa vigente, delle regole stabilite dal Modello, del Codice Etico e delle altre norme interne aziendali, mantenendosi aggiornati sull'evoluzione normativa;
- ispirarsi a criteri di trasparenza nell'esercizio dell'attività aziendale e nella scelta dei partner finanziari;
- assicurare la tracciabilità delle fasi del processo decisionale relativo ai rapporti finanziari e societari con soggetti terzi, garantendo la possibilità di ricostruire ex post, con esattezza, sia il percorso decisionale sia quello formale del flusso finanziario dal punto di partenza al punto di arrivo;
- conservare la documentazione a supporto delle operazioni finanziarie e societarie, adottando tutte le misure di sicurezza necessarie.

Ai fini dell'attuazione dei comportamenti di cui sopra:

- ai soggetti che effettuano operazioni di natura finanziaria o societaria per conto della Fondazione devono essere formalmente conferiti specifici poteri con apposita delega;
- tutte le operazioni di natura commerciale, finanziaria e societaria derivanti da rapporti continuativi ed occasionali con soggetti terzi (ad esclusione degli Intermediari Finanziari) devono essere precedute da un'adeguata attività di verifica volta ad accertare l'assenza del rischio di coinvolgimento nella commissione dei reati di riciclaggio, ricettazione ed impiego di denaro, beni o utilità di provenienza illecita, attraverso una chiara identificazione di:
  - controparte;
  - ove ciò sia possibile, accertamento della provenienza dei beni ricevuti;
  - scopo, natura e struttura dell'operazione;
  - valore dell'operazione;
- tutti gli incassi e i pagamenti derivanti da rapporti di collaborazione con terzi fornitori sono regolati esclusivamente attraverso il canale bancario salvo spese di modico valore;
- i pagamenti in contanti devono essere limitati nel numero e per un importo unitario massimo di 50 euro, dovendo essere adeguatamente documentati e monitorati; nessun tipo di pagamento può essere effettuato in natura;
- coloro che svolgono una funzione di controllo e supervisione su adempimenti connessi all'espletamento delle suddette attività devono porre particolare attenzione all'attuazione degli adempimenti stessi e riferire immediatamente all'OdiV eventuali situazioni di irregolarità.

#### 8.4. I controlli dell'Organismo di Vigilanza

L'OdiV effettua periodicamente controlli a campione sulle attività connesse ai "processi sensibili" diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello. A tal fine, all'OdiV viene garantito libero accesso a tutta la documentazione sociale rilevante e può attivarsi con specifici controlli a seguito delle segnalazioni ricevute.

In particolare, è compito dell'OdiV:

- verificare l'emanazione e l'aggiornamento da parte della Fondazione di istruzioni standardizzate relative agli atteggiamenti da assumere nell'ambito delle attività a rischio e, in particolare, nei rapporti con i fornitori;
- verificare periodicamente il sistema di deleghe in vigore, raccomandando delle modifiche nel caso in cui il potere di gestione o la qualifica non corrispondano ai poteri di rappresentanza conferiti al responsabile interno od ai sub responsabili;
- verificare il rispetto e la corretta applicazione delle prescrizioni previste nei processi sensibili da parte di tutti i soggetti aziendali;
- verificare periodicamente, con il supporto delle altre funzioni competenti, la validità delle procedure finalizzate a:
  - l'osservanza da parte dei Destinatari delle disposizioni del Decreto;
  - l'attuazione di meccanismi sanzionatori qualora si accertino violazioni delle prescrizioni;

- indicare ai dirigenti le opportune integrazioni agli attuali sistemi gestionali delle risorse finanziarie, con l'introduzione di eventuali accorgimenti suscettibili di rilevare l'esistenza di eventuali flussi finanziari atipici e connotati da maggiori margini di discrezionalità rispetto a quanto ordinariamente previsto.

## 9. REATI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE

### 9.1. Quadro di riferimento

I reati richiamati nell'art. 25 novies del Decreto - presupposto della responsabilità amministrativa dell'ente e forieri di pesanti sanzioni pecuniarie ed anche interdittive - sono definiti dalla Legge n. 633 del 22/04/1941, denominata "Protezione del diritto d'autore e di altri diritti connessi al suo esercizio".

Per *diritto d'autore* si intende:

- in senso soggettivo, l'insieme dei diritti e delle facoltà che l'ordinamento giuridico riconosce all'autore delle opere dell'ingegno aventi carattere creativo, e
- in senso oggettivo, come il complesso delle norme giuridiche che regolano l'esercizio e la durata di questi diritti e ne assicurano la protezione; in questo senso, le opere protette dalla legge sul diritto d'autore sono tutte le opere di carattere creativo che appartengono alla letteratura, alla musica, alle arti figurative, all'architettura, al teatro ed alla cinematografia ma, anche, i programmi per elaboratore e le banche di dati che, per la scelta o la disposizione del materiale, costituiscono una creazione intellettuale dell'autore.

Allo scopo di fornire elementi utili all'identificazione del rischio e allo sviluppo di ipotesi di miglioramento:

- per ciascun reato è stata valutata la sua applicabilità o meno nell'ambito delle attività in via di sviluppo nella Fondazione, con un'analisi delle aree coinvolte e dei ruoli di responsabilità in essa inclusi;
- sono state individuate le possibili condotte illecite e di conseguenza gli eventuali reati, nei principali processi operativi;
- sono stati identificati e descritti i punti di controllo opportuni e ne è stata fornita valutazione rispetto alla mitigazione dei rischi individuati.

Quanto sopra con l'obiettivo di fare in modo che tutto il personale che utilizza le risorse informatiche della Fondazione si attenga a regole di condotta conformi ai principi qui prescritti, al fine di prevenire il verificarsi di reati in violazione della legge sul diritto d'autore; in particolare, si intende:

- fornire un elenco dei principi generali, nonché dei principi procedurali specifici cui i soggetti, in relazione al tipo di rapporto in essere con la Fondazione, sono tenuti ad attenersi ai fini di una corretta applicazione del Modello;
- fornire all'OdiV ed ai referenti delle altre funzioni aziendali, chiamati a cooperare con lo stesso, gli strumenti operativi per la concreta attuazione del Modello e per il relativo esercizio delle attività di controllo, monitoraggio e verifica previste.

Oltre alle regole di cui al presente Modello, i soggetti interessati devono in generale conoscere e rispettare, con riferimento alle attività svolte, le regole ed i principi contenuti nei seguenti documenti:

- Statuto,

- Codice Etico,
- Regolamento per la disciplina dei conflitti d'interesse
- Altri regolamenti adottati dalla Fondazione.

## 9.2 Reati in materia di diritto d'autore richiamati nel Decreto

I reati in materia di violazione del diritto d'autore richiamati dall'art. 25-novies del Decreto, che stabilisce le relative sanzioni in termini di responsabilità amministrativa dell'ente, sono identificati dai seguenti articoli della legge 22 aprile 1941, n. 633:

- *art. 171, comma 1 lett. a) bis*: messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa; tale comma tutela l'interesse patrimoniale dell'autore dell'opera il quale potrebbe vedersi ridurre le aspettative di guadagno in caso di libera circolazione della propria opera sulla rete telematica;
- *art. 171, comma 3*: reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione, qualora risulti offeso l'onore o la reputazione del titolare dell'opera, possibilmente lesi dall'usurpazione della paternità dell'opera ovvero dalla mutilazione o altra modificazione dell'opera stessa; per quanto riguarda la responsabilità amministrativa dell'ente, i reati di cui al comma 1 lettera a) bis e comma 3) potrebbero, ad esempio, essere commessi nell'interesse della Fondazione qualora venissero caricati sul sito web aziendale dei contenuti coperti dal diritto d'autore;
- *art. 171-bis, comma 1*: abusiva duplicazione, al fine di trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere arbitrariamente o eludere i dispositivi di protezione di programmi per elaboratori;
- *art. 171-bis, comma 2*: riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati, al fine di trarne profitto, estrazione o reimpiego della banca dati, distribuzione, vendita o concessione in locazione di banche di dati; la terminologia "al fine di trarne profitto" estende il campo di applicazione della norma, a partire dal 2000, a quelle condotte che comportano anche solo un mero risparmio di costi non sostenuti per l'acquisto di copie regolari del software o banche dati; dal punto di vista della responsabilità amministrativa dell'ente, tale reato potrebbe essere commesso nell'interesse della Fondazione qualora:
  - venissero utilizzati, per scopi connessi all'attività lavorativa, programmi non originali, al fine di ottenere un risparmio sui costi derivanti dall'acquisizione della licenza d'uso del software originale o della banca di dati;
  - venissero duplicati abusivamente programmi per elaboratore in numero superiore rispetto alle licenze acquisite, al fine di ottenere un risparmio dei costi delle licenze;
- *art. 171-ter*: abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio di dischi, nastri o supporti analoghi o ogni altro supporto contenente fonogrammi

o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali, multimediali, anche se inserite in opere collettive o composite o banche dati; riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa; l'articolo punisce anche le condotte illecite commesse via Internet quando queste siano caratterizzate dal fine di lucro, restando necessario che l'uso non sia personale bensì travalichi l'ambito del godimento puro da parte di un singolo utente (tale condotta è infatti punibile ai sensi dell'art. 171); stante l'ambito di attività della Fondazione, sembra possa essere difficilmente commesso tale reato nell'interesse o a vantaggio della medesima;

- *art. 171-septies*: mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione; il reato in questione si realizza quando i produttori o importatori dei supporti, non soggetti al contrassegno di SIAE, non comunicano alla stessa SIAE entro 30 gg dalla data di immissione in commercio sul territorio nazionale o di importazione i dati necessari per la univoca identificazione dei supporti medesimi ovvero quando questi soggetti dichiarano falsamente di avere assolti gli obblighi di contrassegno; tale fattispecie di reato non è applicabile alle attività della Fondazione che né produce né commercializza supporti di memorizzazione;
- *art. 171-octies*: fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale; stante l'ambito di attività della Fondazione, tale fattispecie di reato non appare applicabile.

### 9.3. Potenziati attività a rischio

Alla luce degli articoli sopra elencati si evince che le attività della Fondazione valutate come più esposte a rischio di reati in violazione delle norme suddette sono quelle di seguito elencate:

- attività svolte con l'utilizzo dei sistemi informativi aziendali, del servizio di posta elettronica e accesso alla rete Internet;
- attività che comportano la gestione dei sistemi informativi aziendali, incluse le singole Postazioni di Lavoro, al fine di garantirne il corretto funzionamento e manutenzione;
- attività connesse all'utilizzo di software e banche dati;
- attività connesse alla gestione dei contenuti del sito web della Fondazione;
- attività connesse alla gestione delle licenze software.

Il rischio di incorrere nei comportamenti descritti negli articoli sopra esposti, a vantaggio o nell'interesse dell'ente, è mitigato dalla formalizzazione di procedure documentate, diffuse internamente, recanti le regole da rispettare per evitare di incorrere in comportamenti illeciti che potrebbero chiamare in causa la responsabilità dell'ente per violazione delle norme sul diritto d'autore; in effetti, il personale ha la possibilità di accedere, senza alcuna restrizione di carattere tecnologico, tramite la Postazione di Lavoro (desktop o laptop), messa a

disposizione dalla Fondazione per compiere le attività lavorative, alla rete Internet ed a servizi di comunicazione elettronica.

#### 9.4. Principi generali di comportamento

Con l'obiettivo di sensibilizzare il personale ad un consono utilizzo delle risorse informatiche al fine di evitare di incorrere, anche involontariamente, in violazione delle norme sul diritto d'autore, sono definiti i seguenti principi generali di comportamento:

- evitare di utilizzare, nella creazione ed aggiornamento del sito web della Fondazione, materiale reperito in rete (es.: fotografie, immagini, disegni, elementi grafici, testi), salvo espressa autorizzazione dell'autore;
- evitare di modificare (es.: adattamenti, riduzioni, traduzioni, aggiunte, variazioni) materiale reperito in rete (es.: fotografie, immagini, disegni, elementi grafici, testi, musiche), nella creazione ed aggiornamento del sito web della Fondazione, salvo espressa autorizzazione dell'autore;
- è consentito il riassunto, citazione o riproduzione di brani o parti di opere letterarie a scopo di studio, discussione, documentazione o insegnamento: nel fare questo è però necessario citare sempre l'autore e la fonte.

##### 9.4.1. Gestione delle licenze software

Sul tema della gestione delle licenze d'uso di software proprietario, semilibero e commerciale utilizzato in Fondazione, sono definite le seguenti regole di comportamento per il personale:

- prevenire l'utilizzo, da parte del personale, di software non autorizzato e/o in violazione della licenza d'uso;
- prevenire la duplicazione, utilizzo e diffusione di software in violazioni della legge sul diritto d'autore e diritti connessi;
- gestire efficacemente le copie licenziate del software proprietario utilizzato in Fondazione;
- prevenire l'introduzione di software malevolo che potrebbe derivare da un uso incontrollato di software;
- in generale, prevenire la commissione di reati in violazione della legge sul diritto d'autore, che potrebbero comportare la responsabilità amministrativa della Fondazione ai sensi del Decreto.

Gli ambiti di responsabilità dei soggetti coinvolti – specificamente i dipendenti utilizzatori – comprendono il rispetto delle seguenti regole:

- utilizzare correttamente il software installato sulla Postazione di Lavoro in dotazione;
- richiedere sempre formale autorizzazione all'installazione di nuovo software sul proprio PC, al proprio Responsabile di riferimento;
- dichiarare l'eventuale disinstallazione di un software dal proprio PC al fine di "liberare" eventuali licenze;
- rispettare la normativa vigente in materia di tutela del diritto d'autore, che regola anche l'utilizzo del software per elaboratore e delle banche di dati;

- non riprodurre ed utilizzare sulla propria Postazione di Lavoro software proprietario per il quale:
  - se acquistato dalla Fondazione, non sia stata ottenuta autorizzazione dal Responsabile di riferimento;
  - se acquistato da terzi, non si disponga di regolare licenza o evidenza di regolarità per quanto riguarda la concessione d'uso;
- utilizzare il software secondo le modalità previste nella licenza d'uso dal titolare dei diritti d'autore sul software o sulla banca di dati.

E', inoltre, prevista l'introduzione della figura del *Referente del software*, titolare dei seguenti compiti:

- controllare la situazione delle licenze, per provvedere al tempestivo riordino in caso di necessità;
- custodire correttamente il software (cd o disco di rete) per l'installazione;
- supportare, dal punto di vista tecnico, l'Area Acquisti e in generale il sistema di gestione licenze;
- gestire il piano acquisti relativo alle licenze del software di cui è referente e mantenere aggiornato il sistema di gestione licenze in merito al numero di licenze acquistate;
- definire le modalità di distribuzione del software e delle eventuali chiavi di accesso.

Infine, ogni Responsabile di riferimento ha il compito di:

- vigilare sul rispetto delle norme di legge in materia di "diritto d'autore" nell'utilizzo del software proprietario;
- autorizzare o rifiutare formalmente l'acquisto e l'installazione di un software richiesto dal personale.

La Fondazione non vieta a priori l'utilizzo delle tecnologie di comunicazione elettronica (rete Internet) in quanto mezzo che potrebbe essere utilizzato per veicolare contenuti illeciti; vieta, invece, l'utilizzo degli strumenti messi a disposizione dalla rete Internet per veicolare contenuti illeciti (es.: software, banche dati, file musicali, video), in violazione della legge sul diritto d'autore. Sono, pertanto, definite le seguenti regole per il personale:

- non mettere a disposizione del pubblico, tramite reti telematiche, connessioni e strumenti di qualsiasi genere, un'opera dell'ingegno protetta o parte di questa, senza averne diritto (ad esempio, tramite pubblicazione nel sito della Fondazione),
- non duplicare, importare, distribuire, vendere o dare in locazione, abusivamente per trarne profitto, software per elaboratore a scopo commerciale o imprenditoriale;
- non riprodurre, trasferire su altro supporto, distribuire, comunicare, presentare o dimostrare in pubblico, estrarre o reimpiegare i contenuti della banca dati, distribuire, vendere o dare in locazione i contenuti di una banca dati, al fine di trarne profitto, in violazione delle disposizioni della legge sul diritto d'autore;
- comprendere che comportamenti non conformi potrebbero esporre la Fondazione alla responsabilità amministrativa delle imprese secondo il Decreto.

#### 9.4.2. Utilizzo della Postazione di Lavoro per la posta elettronica e i servizi Internet

E' un onere a carico del Datore di Lavoro quello di garantire la funzionalità ed il corretto sull'utilizzo dei PC aziendali e dei servizi da questi disponibili (accesso alla rete Internet, posta elettronica, file server di dominio) da parte del personale, attraverso una chiara definizione delle modalità d'uso consono di tali strumenti nell'organizzazione dell'attività lavorativa. In effetti, proprio tramite l'uso della posta elettronica e della rete Internet è possibile incorrere nei reati in tema di diritto d'autore e, pertanto, sono fissate le seguenti regole di comportamento:

- non utilizzare il servizio di posta elettronica per immettere in rete materiale in violazione della vigente normativa sul diritto d'autore;
- evitare il download dalla rete Internet di file e programmi non pertinenti rispetto alla propria mansione aziendale (es.: file musicali, opere cinematografiche) o in violazione della legge sul diritto d'autore;
- non inserire, sui siti web della Fondazione, dati, immagini o altro materiale coperto dal diritto d'autore senza avere ottenuto le necessarie autorizzazioni;
- seguire adeguati accorgimenti per evitare di incorrere in codice malevolo e virus, nella navigazione in Internet e nell'utilizzo della posta elettronica, che potrebbero danneggiare il sistema informativo aziendale.

Specifica attenzione deve essere prestata nella rimozione del software commerciale dai supporti magnetici dismessi, nel caso sia prevista dalla licenza d'uso del fornitore.

#### 9.4.3. Formazione e addestramento del personale

E' responsabilità del Direttore pianificare attività di formazione e addestramento per i neoassunti e per tutto il personale che ha accesso ed utilizza le risorse informatiche aziendali, al fine di diffondere la cultura della sicurezza con particolare riferimento a:

- la definizione dei comportamenti considerati accettabili per un corretto utilizzo di software e banche dati, e
- la diffusione della consapevolezza sui rischi derivanti da un utilizzo improprio delle risorse informatiche aziendali.

Le attività di formazione e di training on the job sono tracciate, a livello di singolo dipendente, per ottenere un quadro esaustivo di conoscenza sui livelli raggiunti in tema di addestramento, qualificazione e consapevolezza del personale.

Infine, è previsto il tracciamento automatico di alcune informazioni (log) relative alle attività svolte dal lavoratore nell'utilizzo della posta elettronica e delle navigazioni in Internet, con l'obiettivo di poter analizzare le cause di anomalie, incidenti di sicurezza e comportamenti non conformi alle regole sull'utilizzo degli strumenti di lavoro aziendali; ciò nel rispetto dell'informativa sulla privacy fornita al personale ai sensi dell'art. 13 del D.lgs.196/2003.

### 9.5. I controlli dell'Organismo di Vigilanza

Fermo restando quanto già previsto nella parte generale del Modello sull'OdiV, compiti ulteriori dell'Organo, in relazione all'osservanza del Modello per quanto riguarda i reati di cui all'art. 25 nonies, sono:

- svolgere verifiche periodiche, direttamente o con la collaborazione di consulenti tecnici esterni esperti, sul rispetto della normativa sul diritto d'autore e valutarne l'efficacia nel prevenire la commissione dei Reati di cui all'art. 25 nonies del Decreto;
- segnalare alla Direzione la necessità di aggiornare e migliorare le istruzioni operative comportamentali e le misure di sicurezza in vigore, finalizzate alla minimizzazione dei rischi di reato, qualora vengano rilevate violazioni significative delle norme in materia di violazione del diritto d'autore o in occasione di modifiche dell'organizzazione aziendale ed al progresso scientifico e tecnologico;
- stimolare, ove si rilevino aree di vulnerabilità, la predisposizione di procedure operative standardizzate ulteriori relative a regole comportamentali da seguire nell'ambito delle attività a rischio individuate;
- ricevere ed analizzare eventuali segnalazioni di presunte violazioni del Modello, in materia di diritto d'autore, ed effettuare gli accertamenti ritenuti necessari per verificare la veridicità delle segnalazioni ricevute.

Il Direttore curerà di acquisire ed analizzare le informazioni contenute nelle relazioni periodiche all'OdiV, al fine di verificare la presenza di informazioni su eventi rilevanti attinenti alle aree a rischio in materia di diritto d'autore.

## 10. REATI AMBIENTALI

### 10.1. Le tipologie dei reati ambientali

I reati ambientali richiamati nell'art. 25 undecies del Decreto - presupposto della responsabilità amministrativa dell'ente e forieri di pesanti sanzioni pecuniarie ed anche interdittive - sono definiti dalle norme di riferimento di seguito specificate.

#### 10.1.1. Codice penale

- Uccisione, distruzione, cattura, prelievo, detenzione di esemplari di specie animali o vegetali selvatiche protette (art. 727-bis)
- Distruzione o deterioramento di habitat all'interno di un sito protetto (art. 733-bis)

#### 10.1.2. Decreto Legislativo 152/2006 (Codice dell'Ambiente)

- *Art. 137 Cod. Amb.:* risultano rilevanti per le finalità di cui al Decreto le seguenti condotte:
  - scarico di acque reflue industriali senza autorizzazione o con autorizzazione sospesa o revocata;
  - scarico di acque industriali eccedenti limiti tabellari;
  - violazione del divieto di scarico sul suolo, nel suolo e nelle acque sotterranee;
  - violazione del divieto di scarico in mare da parte di navi e aereomobili di sostanze vietate.
- *Art. 256 Cod. Amb.:* sanziona penalmente una pluralità di condotte che, configurandosi prevalentemente come violazione di disposizioni normative relative alla gestione di rifiuti, sono potenzialmente lesive dell'ambiente:
  - gestione non autorizzata di rifiuti,
  - gestione di discarica non autorizzata,
  - miscelazione di rifiuti pericolosi,
  - deposito temporaneo di rifiuti sanitari pericolosi,
  - violazione dei limiti temporali o quantitativi previsti dall'art. 8 del D.P.R. 254/2003, in relazione al deposito temporaneo di rifiuti sanitari pericolosi.
- *Art. 257 Cod. Amb.:* riguarda la disciplina penale della bonifica dei siti, prevede due distinte fattispecie di reato:
  - l'omessa bonifica del sito inquinato;
  - la mancata comunicazione dell'evento inquinante alle autorità competenti secondo le modalità indicate dall'art. 242 Cod. Amb.
- *Art. 258 comma 4, secondo periodo Cod. Amb.:* riguarda la falsità nella predisposizione di un certificato di analisi dei rifiuti - in termini di false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti - nonché l'uso di un certificato falso durante il trasporto.

- *Art. 259 Cod. Amb.:* riguarda il traffico illecito e le spedizioni transfrontaliere dei rifiuti.
- *Art. 260 primo e secondo comma Cod. Amb.:* riguarda le attività organizzate per il traffico illecito di rifiuti ovvero chi, per conseguire un ingiusto profitto, con più operazioni e attraverso l'allestimento di mezzi e attività continuative organizzate, cede, riceve, trasporta, esporta, importa, o comunque gestisce abusivamente ingenti quantitativi di rifiuti; il reato è aggravato qualora i rifiuti siano ad alta radioattività.
- *art. 260 bis Cod. Amb.:* riguarda il Sistema informatico di controllo della tracciabilità dei rifiuti, per cui è punito colui che, nella predisposizione di un certificato di analisi di rifiuti, utilizzato nell'ambito del sistema di controllo della tracciabilità dei rifiuti, fornisce false indicazioni sulla natura, composizione e caratteristiche chimico-fisiche dei rifiuti e a chi inserisce un certificato falso nei dati da fornire ai fini della tracciabilità dei rifiuti; sono inoltre puniti i trasportatori che:
  - omettono di accompagnare il trasporto di rifiuti pericolosi con la copia cartacea della scheda di movimentazione del SISTRI e con la copia del certificato analitico che identifica le caratteristiche dei rifiuti;
  - fanno uso di un certificato di analisi di rifiuti contenente indicazioni false sulla natura, composizione e caratteristiche chimico-fisiche dei rifiuti trasportati, e
  - accompagnano il trasporto di rifiuti – pericolosi e non pericolosi - con una copia cartacea della scheda SISTRI-AREA Movimentazione fraudolentemente alterata.
- *art. 279 Cod. Amb.:* riguarda l'emissione in atmosfera di gas inquinanti oltre i limiti consentiti

### 10.1.3. Prevenzione dell'effetto serra

- *Regolamento (CE) n.842/2006 del Parlamento Europeo e del Consiglio del 17 maggio 2006;* il c.d. Regolamento F-Gas ha l'obiettivo di ridurre le emissioni di gas fluorurati ad effetto serra, contemplate dal Protocollo di Kyoto.
- *Legge 28 dicembre n. 549 del 1993 recante "Misure a tutela dell'ozono stratosferico e dell'ambiente"* che, all'art. 3 comma 6, dispone in merito alle violazioni delle disposizioni relative alla produzione, consumo, importazione, esportazione, detenzione e commercializzazione di sostanze lesive.

### 10.2. Potenziati Aree a rischio

In relazione ai reati e alle condotte criminose sopra esplicitate, le aree ritenute più specificamente a rischio risultano essere le seguenti:

- attività di selezione e qualificazione dei fornitori, in particolare per l'attività di conferimento, trasporto e smaltimento dei rifiuti;
- gestione interna dei rifiuti prodotti nonché gestione degli adempimenti e dichiarazioni obbligatorie per legge in materia ambientale;

- gestione operativa delle manutenzioni dei sistemi di condizionamento dei locali e delle sale macchine in riferimento all'applicazione del DPR 43/2012 in materia di F-GAS.

### 10.3. Principi generali di comportamento e di attuazione

Affinché tutti i destinatari si attengano - nella misura in cui sono coinvolti nello svolgimento delle attività nelle Aree a Rischio - a regole di condotta volte a prevenire e impedire il verificarsi dei reati previsti nel Decreto, le specifiche di seguito proposte servono a:

- fornire un elenco dei principi generali nonché dei principi procedurali specifici cui i destinatari sono tenuti ad attenersi per una corretta applicazione del Modello;
- fornire all'OdiV e ai responsabili delle funzioni aziendali chiamati a cooperare con lo stesso, gli strumenti operativi necessari al fine di poter esercitare le attività di controllo, monitoraggio e verifica previsti.

In generale, tutti i destinatari sono tenuti al rispetto dei principi di comportamento contenuti nei diversi documenti organizzativi della Fondazione, fra i quali si citano:

- normativa vigente in materia ambientale;
- organigramma aziendale e schemi organizzativi;
- politica di sicurezza e ambiente;
- regole, procedure ed istruzioni operative in tema di qualificazione e scelta dei Fornitori;
- linee guida, sistemi di gestione, procedure, istruzioni operative e note interne in materia di sicurezza ed igiene sul lavoro, gestione ambientale e dei rifiuti.
- Modello organizzativo e Codice etico.

### 10.4. Principi procedurali specifici

Di seguito i principi procedurali specifici volti a prevenire la commissione dei Reati Ambientali in relazione alla Gestione dei Rifiuti; la Fondazione, attraverso il Servizio di Prevenzione e Protezione a gestione diretta, ovvero attribuendo a contraenti esterni specializzati in materia:

- si adopera per una gestione dei rifiuti orientata al recupero, al reimpiego e al riciclaggio dei materiali, nel rispetto delle norme in materia ambientale;
- definisce i principali adempimenti da adottare internamente in merito alla Gestione delle diverse tipologie rifiuti - pericolosi e non pericolosi;
- provvede alla classificazione dei rifiuti prodotti nell'ambito delle attività svolte in conformità a quanto stabilito dalle disposizioni legislative vigenti e dalle autorità competenti e a tal fine informa e fornisce adeguata formazione al personale delle sedi produttive di rifiuti sulle base delle rispettive attribuzioni;
- affida le attività di raccolta, trasporto, recupero e smaltimento dei rifiuti esclusivamente ad imprese autorizzate e nel rispetto delle procedure aziendali relative alla qualificazione dei Fornitori;
- se applicabile, garantisce che la sede produttiva di rifiuti tenga regolarmente il registro di carico e scarico e che lo stesso, unitamente ai formulari identificativi

del rifiuto, siano compilati in modo corretto e veritiero, astenendosi dal porre in essere operazioni di falso ideologico o materiale (ad esempio in relazione alle informazioni sulle caratteristiche qualitative o quantitative dei rifiuti);

- in conformità a quanto previsto dalle disposizioni in materia ambientale, compila accuratamente e regolarmente il Modello Unico di Dichiarazione Ambientale;
- istituisce presidi idonei a garantire il rispetto delle disposizioni normative relative al deposito dei rifiuti ed in particolare delle modalità e dei limiti quantitativi e temporali tempo per tempo vigenti;
- si impegna a garantire che le procedure aziendali relative alla gestione dei rifiuti, siano sottoposte ad un costante monitoraggio da parte delle funzioni aziendali preposte al fine di valutare periodicamente l'opportunità di aggiornamenti in ragione di interventi normativi in materia ambientale;
- vigila costantemente sulla corretta Gestione dei Rifiuti segnalando eventuali irregolarità alla Direzione (es.: manomissione dei documenti di classificazione, sospetto di abbandono dei rifiuti da parte del trasportatore in discariche abusive) al fine di porre in essere le conseguenti azioni di tipo amministrativo e contrattuale, oltre che le eventuali azioni di tipo legale dinanzi alle competenti autorità.

Il Servizio di Prevenzione e Protezione, inoltre, cura l'adempimento degli obblighi derivanti dall'applicazione del DPR 43/2012, recante l'attuazione del predetto Regolamento F-Gas, secondo cui, entro il 31 maggio di ogni anno, gli operatori delle applicazioni fisse di refrigerazione, condizionamento d'aria e pompe di calore, nonché dei sistemi fissi di protezione antincendio contenenti 3 kg o più di gas fluorurati ad effetto serra devono presentare una dichiarazione contenente informazioni riguardanti la quantità di emissioni in atmosfera relativi all'anno precedente sulla base dei dati contenuti nel relativo registro di impianto.

#### 10.5. Istruzioni e verifiche dell'Organo di Vigilanza

I compiti di vigilanza dell'OdiV in relazione all'osservanza del Modello per quanto concerne i Reati Ambientali sono i seguenti:

- svolgere verifiche periodiche sul rispetto delle disposizioni in materia e valutare periodicamente la loro efficacia a prevenire la commissione dei Reati dove previsti; l'OdiV, avvalendosi eventualmente della collaborazione di consulenti tecnici competenti in materia, condurrà una periodica attività di analisi sulla funzionalità del sistema preventivo adottato e proporrà alla Direzione eventuali azioni migliorative o modifiche qualora vengano rilevate violazioni significative delle norme sui Reati Ambientali;
- esaminare eventuali segnalazioni di presunte violazioni ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

Viene garantita l'istituzione di flussi informativi tra l'OdiV e la Direzione e la funzione aziendale coinvolta che, in ogni caso, potranno essere sentiti dall'OdiV ogni volta ritenuto opportuno. L'informativa all'OdiV dovrà essere data senza indugio nel caso in cui si verificano violazioni ai principi procedurali specifici; è, altresì, attribuito all'OdiV il potere di accedere o di richiedere ai propri delegati di accedere a tutta la documentazione e ai locali della Fondazione rilevanti per lo svolgimento dei propri compiti.

## 11. IMPIEGO DI LAVORATORI IRREGOLARI

### 11.1. Reati inerenti all'impiego di lavoratori irregolari

In sintesi, l'Ente che occupa alle proprie dipendenze lavoratori stranieri privi del permesso di soggiorno, ovvero il cui permesso sia scaduto e del quale non sia stato chiesto, nei termini di legge, il rinnovo, revocato o annullato, è perseguibile ai sensi del Decreto, se i lavoratori occupati sono (circostanze alternative tra di loro):

- in numero superiore a tre;
- minori in età non lavorativa;
- esposti a situazioni di grave pericolo con riferimento alle prestazioni da svolgere e alle condizioni di lavoro.

I reati e le sanzioni di cui trattasi sono identificati da diverse fonti normative a cui rimandano l'art. 2 del D. Lgs. 16 luglio 2012 n. 109 e l'art. 25 *duodecies* del Decreto, rubricato come "Impiego di cittadini di Paesi terzi il cui soggiorno è irregolare".

In particolare, si evidenzia che:

- il c.d. "*Reato di caporalato*", previsto dall'art. 603 *bis* del Codice Penale (utilizzo di lavoratori, reclutati tramite intermediari non autorizzati, c.d. "caporali", già soggiornanti in Italia ed in possesso di regolare permesso di soggiorno) non è direttamente richiamato dal Decreto, ad eccezione di eventuali circostanze aggravanti conducenti al più grave reato di "Riduzione in schiavitù" di cui all'art. 600 c.p. e art. 25 *quinquies* del Decreto o dell'ulteriore reato di "Associazione per delinquere" di cui all'art. 416 c.p. e art. 24 *ter* del Decreto; resta ferma, in ogni caso, la responsabilità penale dell'intermediario e, presumibilmente, del Datore di Lavoro;
- in tema di *affidamento, gestione e vigilanza sui contratti d'appalto, d'opera e somministrazione*, la responsabilità amministrativa dell'Ente per il reato di impiego di lavoratori irregolari da parte di subappaltatori non è autonomamente configurabile, ai sensi del Decreto, anche a carico dell'appaltatore; tuttavia, poiché vige l'istituto della responsabilità solidale - per cui l'appaltatore risponde in solido con il subappaltatore sia per i trattamenti retributivi che per i contributi previdenziali e assicurativi (escluso l'obbligo per le sanzioni civili delle quali risponde solo il responsabile dell'adempimento) - queste attività presentano un chiaro rilievo in termini di efficace contrasto all'impiego di lavoratori stranieri irregolari.

### 11.2. Potenziabili aree a rischio

I settori, processi e attività esposti maggiormente a rischio, per i reati di impiego di lavoratori irregolari, riguardano:

- la selezione e assunzione di lavoratori stranieri;
- la stipula e gestione di contratti e ordini di acquisto;
- l'affidamento, gestione e vigilanza sui contratti d'appalto, d'opera e somministrazione.

I settori della Fondazione maggiormente interessati sono:

- il Presidente del Consiglio di Amministrazione,
- il Direttore,
- il Servizio di Prevenzione e Protezione, con i Preposti per la Sicurezza,
- l'area Risorse Umane e Organizzazione, nella sua progressiva realizzazione.

### 11.3. Principi di riferimento generali

Il sistema organizzativo in generale della Fondazione – nella sua progressiva evoluzione dimensionale - deve essere dotato di strumenti e procedure organizzativi caratterizzati dai seguenti elementi:

- separazione all'interno di ciascun processo tra il soggetto che assume la decisione, il soggetto che esegue tale decisione ed il soggetto al quale è affidato il controllo del processo (c.d. segregazione delle funzioni);
- traccia scritta di ciascun passaggio rilevante del processo (c.d. tracciabilità);
- adeguato livello di formalizzazione.

Con specifico riferimento ai reati di impiego di lavoratori irregolari, facendo salvo il rigoroso rispetto del Codice Etico, delle norme e delle prassi aziendali, la normativa vigente deve essere rigorosamente rispettata in tutte le fasi propedeutiche all'assunzione, quali:

- la presentazione della domanda di nulla osta all'assunzione di lavoratore straniero residente all'estero,
- il rilascio di nulla osta all'assunzione,
- la richiesta e rilascio del visto di ingresso,
- l'ingresso in Italia,
- gli obblighi di comunicazione per l'assunzione,
- la richiesta del rinnovo di permesso di soggiorno prima della scadenza,
- l'assunzione di un lavoratore straniero già soggiornante in Italia,
- il divieto di assunzione di un lavoratore straniero privo di permesso di soggiorno,
- la validità del permesso di soggiorno per lo straniero che perde il lavoro.

Circa l'affidamento, la gestione e la vigilanza dei contratti d'appalto, d'opera e somministrazione - quando tali attività saranno realizzate direttamente dalla Fondazione - dovranno essere attuate specifiche procedure per:

- la verifica preliminare dell'idoneità tecnico professionale delle imprese esecutrici e dei lavoratori autonomi accedenti al cantiere, ai sensi di quanto previsto dall'art. 26, comma 1, lettera a) del D. Lgs. 81/08 e ss.mm.ii. (c.d. Testo Unico della Sicurezza);
- l'acquisizione dell'elenco aggiornato degli addetti presenti in cantiere per l'esecuzione dei lavori affidati all'impresa esecutrice e relativa verifica documentale di regolarità;

- la vigilanza sull'effettivo personale dell'impresa esecutrice presente in cantiere con verifica delle generalità, ovvero dei dati indicati nei tesserini di riconoscimento a fronte di quelli dichiarati e ufficialmente comunicati attraverso l'elenco di cui sopra.

#### 11.4. I controlli dell'Organismo di Vigilanza

Fermo restando il potere discrezionale dell'OdiV di attivarsi con specifici controlli a seguito delle segnalazioni ricevute, l'OdiV effettua periodicamente controlli a campione sulle attività connesse ai processi sensibili ai reati di impiego di lavoratori irregolari, diretti a verificare la loro corretta esecuzione in relazione ai principi espressi nel presente documento e alle procedure interne in essere.

Per l'effettuazione di tali controlli periodici, l'OdiV si avvale, altresì, della collaborazione delle pertinenti funzioni aziendali, mantenendo la libertà di accesso a tutte le attività aziendali e la disponibilità di consultazione e/o acquisizione di tutta la documentazione rilevante.