ISFORT S.p.A.
Istituto Superiore di Formazione e Ricerca per i Trasporti

Via Nizza, 45 – 00198 Roma
Tel. 06852651 – Fax 0685265246
e-mail: info@isfort.it pec: isfort@arubapec.it sito: www.isfort.it

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO
ai sensi del D.Lgs. n.231 – 8 giugno 2001
PARTE SPECIALE
PRINCIPI E STANDARD DI CONTROLLO

COPIA BETA	01/2020 [X]	data 25/11/2020
COPIA REVISIONATA	02/2021 [X]	data 12/03/2021
COPIA REVISIONATA	03/2021 [X]	data 23/03/2021
COPIA APPROVATA	04/2021 [X]	data 26/03/2021
NUMERO COPIA	…./2021	

Emissione AD	data …26/03/21….	firma …….
Approvazione AD	data …26/03/21….	firma …….
Approvazione ODV	data …26/03/21….	firma …….

Revisione no.	data	intervento	responsabile
01	…/…/…../	……	……
02	…/…/…../	……	……
03	…/…/…../	……	……

SOMMARIO

1. PREMESSE OPERATIVE

Nella Parte Speciale del Modello di organizzazione, gestione e controllo sono definiti, per ogni fattispecie di reato, **i comportamenti generali, specifici e ineludibili**, adottati da Isfort e finalizzati a prevenire il verificarsi di situazioni favorevoli alla commissione dei reati presupposto 231.

La valutazione delle **aree di intervento sistematico e dei processi sensibili aziendali** con specifico riferimento ai reati presupposto di cui al Decreto, è stata effettuata sulla scorta dell'aggiornamento del Decreto medesimo alla data del D.Lgs. 14 luglio 2020, n. 75, e dell'aggiornamento del 19.02.2019, delle Linee Guida (di seguito Linee Guida) redatte dal Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili, con la collaborazione di ABI, Confindustria e Consiglio Forense.

Con tali riferimenti normativi e valutativi, ai fini della redazione del Modello **si è attuato preliminarmente il monitoraggio degli standard di controllo** in essere presso Isfort S.p.A.

È opportuno ricordare che la **funzione esimente del modello 231**, quando il reato sia stato commesso da persone che rivestono funzioni di direzione, amministrazione o controllo dell'azienda o di unità organizzative aziendali, provviste di autonomia funzionale e decisionale, si realizza quando l'azienda dimostra che:

- ha adottato ed efficacemente attuato, prima della commissione del reato, modelli di organizzazione e gestione idonei a prevenire reati della specie di quello verificatosi;
- se è stato affidato a un organismo della società, dotato di autonomi poteri di iniziativa e di controllo, il compito di vigilare sul funzionamento e l'osservanza dei modelli e di curare il loro aggiornamento;
- le persone che hanno commesso il reato hanno eluso, in misura fraudolenta, i modelli di organizzazione e di gestione;
- la direzione e l'organismo di vigilanza non abbiano omesso la vigilanza o l'abbiamo esercitata in misura insufficiente.

Diventa cogente ai fini della funzione esimente, che le fattispecie di commissione di un reato siano state analizzate attentamente così da poter dimostrare che, in caso di reato commesso da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti sopra indicati, l'azienda non è responsabile di carenza di osservanza dai predetti obblighi di direzione e vigilanza.

Elemento essenziale del processo di adeguamento alla norma esimente richiede di:

- prevedere specifici protocolli (i.e. procedure) diretti a programmare la formazione e l'attuazione delle decisioni della società in relazione ai reati da prevenire
- individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione di tali Reati
- prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei Modelli
- introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

Il monitoraggio della situazione in essere ha determinato **l'elaborazione di protocolli e regole, di comportamento**, nel pieno rispetto delle norme vigenti in accordo ai principi e dei valori guida che ispirano il Codice Etico adottato dall'Istituto.

Nella parte Speciale sono definite, per ogni fattispecie di reato, **comportamenti generali, specifici e ineludibili**, finalizzati a prevenire la commissione delle diverse tipologie di reato di cui al Decreto sulla scorta dell'aggiornamento, del 19.02.2019, delle **Linee Guida** (di seguito Linee Guida) **redatte dal Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili, con la collaborazione di ABI, Confindustria e Consiglio Forense**, elaborate per evitare il verificarsi di situazioni favorevoli alla commissione dei reati ex D.lgs. 231/2001.

Su questa base il monitoraggio attuato da Isfort può essere riassunto secondo i seguenti punti fondamentali:

- Individuazione dei processi aziendali al fine di evidenziare le aree di rischio, ovvero i settori ove sia possibile la realizzazione degli eventi pregiudizievoli previsti dal D. Lgs. 231/2001
- predisposizione di un sistema di controllo in grado di prevenire i rischi attraverso l'adozione di appositi protocolli.
  Le componenti più rilevanti, secondo le Linee Guida di cui in precedenza sono:
  - codice etico
  - sistema disciplinare interno
  - sistema organizzativo
  - procedure manuali ed informatiche
  - poteri autorizzativi e di firma
  - sistemi di controllo e gestione
  - modalità di comunicazione e condivisione del personale e sua formazione.

Le componenti del sistema di controllo sono state informate ai seguenti principi:

- applicazione del principio di separazione delle funzioni (nessuno può gestire in autonomia un intero processo)
- verificabilità, documentabilità, coerenza e congruenza di ogni operazione
- documentazione dei controlli
- previsione di un adeguato sistema sanzionatorio per la violazione delle norme del codice etico e delle procedure previste dal modello
- individuazione dei requisiti dell'Organismo di Vigilanza, in base ai principi di autonomia e indipendenza, professionalità, continuità di azione.

È evidente che la non completa applicazione di punti specifici delle Linee Guida non inficia la validità del modello che deve avere un riferimento diretto alla realtà aziendale, considerando le predette Linee Guida come elementi di orientamento generale.

È opportuno precisare, invece, che Isfort con la redazione del modello 231 prosegue il suo impegno di dotarsi di un sistema di ***governance* societaria efficace**, soprattutto in termini di vigilanza sull'applicazione dei principi di buona gestione aziendale nel rispetto dei requisiti di committenti pubblici e privati e degli stakeholders ha approvato ed efficacemente attuato:

- il **Manuale della Qualità (MQ 01.04 2019)**, che sottolinea l'impegno dell'Istituto nel fornire con regolarità e continuità prodotti e servizi che soddisfino i requisiti secondo la normativa UNI EN ISO 9001:2015;
- il **Documento di valutazione d'impatto sulla protezione dei dati** e **Registro dei Trattamenti**, **(DPIA del 15.04.2020)**, in ottemperanza al REGOLAMENTO UE 2016/679, per gestire la raccolta e il trattamento dei dati personali;

- il **Documento di Valutazione dei Rischi (DVR - revisione del 10.10.2019)** per la prevenzione e sicurezza nei luoghi di lavoro a norma del D.Lgs. 81/2008.
- Il **Documento di Valutazione e Gestione del rischio biologico e non intenzionale da Coronavirus negli ambienti di lavoro** - Addendum al DVR del 29.07.2020.

2. AREE DI INTERVENTO SISTEMATICO

Si è proceduto a monitorare, in primo luogo, **le aree di intervento sistematico** dell'Istituto che, in coerenza con la propria missione statutaria di supporto allo sviluppo delle conoscenze e buone pratiche del settore della mobilità, consistono principalmente nella **ricerca** e nella **formazione**.

Per una analisi dettagliata dei processi produttivi aziendali si rinvia al citato **Manuale della Qualità (MQ 01.04 2019)**.

2.a. Ricerca

Nell'ambito dell'area ricerca Isfort produce conoscenze scientifiche nel settore dei trasporti, con la finalità di promuovere una più moderna e diffusa cultura della mobilità, **con l'obiettivo di leggere e interpretare i fenomeni e le tendenze più rilevanti del settore**, identificare i problemi critici e progettare strumenti operativi e modelli di comportamento appropriati per affrontarli.

Le attività di ricerca rientrano nelle competenze e responsabilità della **Direzione Ricerca** dell'Istituto e sono ai **tre Osservatori sulla Mobilità** e ai progetti specifici richiesti di anno in anno. L'elaborazione dei dati dell'Osservatorio "**Audimob**", giunto alla 20a edizione, con gli aggiornamenti delle rilevazioni 2018 e del primo semestre 2019, permette di leggere in profondità le caratteristiche e le dinamiche degli stili e dei comportamenti di mobilità degli italiani.

Le risultanze delle rilevazioni di Isfort su questo tema sono entrate a far parte del **Conto Nazionale dei Trasporti e delle previsioni del Programma Statistico Nazionale** cui l'Istituto invia gli aggiornamenti annuali dell'Osservatorio Audimob, in quanto inserito nel **Sistema Statistico Nazionale - SISTAN** – dell'Istat con provvedimento della Presidenza del Consiglio dei Ministri del 14 marzo 2012. L'Osservatorio Audimob è inserito anche nel Programma Statistico Nazionale 2020 – 2022.

2.b. Formazione

Nell'ambito dell'**area formazione** l'Istituto progetta e realizza interventi finalizzati allo sviluppo della cultura e delle competenze gestionali in imprese e istituzioni operanti nel settore della mobilità, principalmente attraverso **la produzione di servizi di formazione e qualificazione tecnico-professionale del personale**.

In linea di principio **i corsi**, a livello nazionale riservati agli **Operatori qualificati addetti alle mansioni per le attività di sicurezza previste nel trasporto ferroviario** sono competenza della specifica struttura dell'Istituto, di seguito denominata **Direzione Formazione Attività Sicurezza Ferroviaria** (in breve **CdF**) con i ruoli e le responsabilità previsti secondo le Linee Guida **dell'Agenzia Nazionale per la Sicurezza delle Ferrovie**, ANSF, ente pubblico sottoposto ai poteri di indirizzo e vigilanza del Ministro delle infrastrutture e dei trasporti e al controllo della Corte dei Conti.

3. PROCESSI SENSIBILI RELATIVI ALLE AREE A RISCHIO

Con riferimento alle aree di intervento sistematico dell'Istituto, di cui al precedente punto, sono individuati i seguenti **processi sensibili** comuni alle attività dell'organizzazione:

- processo di gestione dei rapporti con enti pubblici o incaricati di pubblico servizio per attività di ricerca
- processo di gestione dei rapporti con enti pubblici o incaricati di pubblico servizio per attività di formazione
- processo di gestione delle risorse umane
- processo commerciale e relazioni con il territorio
- processo di approvvigionamento
- processo di gestione dei sistemi informativi
- processo amministrativo (registrazione, redazione e controllo dei documenti contabili ed extra contabili) e finanziario
- processo di gestione degli investimenti e delle spese realizzati con fondi pubblici
- processo di gestione del contenzioso civile, penale, amministrativo ed ambientale in cui sia parte la p.a.
- processo di gestione dei rapporti con la p.a. per l'ottenimento di licenze o autorizzazioni amministrative

Isfort si attiene alle citate Linee Guida che **prescrivono per ciascun processo sensibile** individuato le modalità di svolgimento delle relative attività ed indica, ove rilevanti, le specifiche procedure cui attenersi prevedendo in particolare:

- protocolli per la formazione e l'attuazione delle decisioni:
  - disposizioni aziendali idonee a fornire principi di riferimento generali per la regolamentazione di ogni processo sensibile
  - poteri di firma e poteri autorizzativi formalizzati verso l'esterno
  - poteri di firma e poteri autorizzativi interni

- standard di controllo, che consentano:
  - segregazione delle attività
  - segregazione chi esegue, chi controlla e chi autorizza

- tracciabilità:
  - l'attività sensibile e i suoi elementi caratterizzanti deve essere tracciata e tracciabile
  - le modalità di gestione delle risorse finanziarie

- gli obblighi di informazione dell'OdV – Organismo di Vigilanza

Le Linee guida dei Dottori Commercialisti, ABI, Confindustria e Consiglio Forense, emanate nel febbraio 2019, hanno suggerito di definire gli standard di controllo della possibilità di commissione di reati presupposto 231

in relazione a comportamenti dell'area del FARE e del NON FARE, specificando in chiave operativa quanto espresso dai principi del Codice Etico per ciascuna fattispecie di reato.

Nell'AREA DEL FARE **definite come prioritarie per Isfort le prescrizioni, i protocolli, le procedure e i comportamenti** che attengono alla responsabilità, principalmente, delle persone apicali dell'azienda, dotate di specifiche attribuzione di poteri e deleghe.

Nell'AREA DEL NON FARE **sono indicati i comportamenti che Isfort ritiene espressamente vietati** e che attengono a tutte le funzioni apicali, i componenti degli organi amministrativi e di controllo, al personale e ai collaboratori continuativi.

Completato il monitoraggio dei singoli standard di controllo ed elaborata una matrice di valutazione del rischio di non compliance, ovvero della probabilità che il modello **non possa avere la peculiare validità di esimente con riguardo ai reati presupposto 231,** si sono identificati i necessari aspetti migliorativi e, quindi, si sono definiti i presenti **principi e standard che Isfort ritiene assolutamente irrinunciabili ai fini della efficacia preventiva e garanzia della condizione esimente**, a norma dell'art. 6, comma 1 del 231/2001, attraverso le misure di seguito descritte, che consentono all'ente di non rispondere dei reati presupposto 231.
Quella che segue è, dunque, la **definizione dei principi e delle regole di condotta** alle quali l'Istituto ritiene di conformarsi, coinvolgendo tutte le funzioni apicali, i dipendenti, i collaboratori, i soggetti esterni che partecipano in diversa misura alle attività aziendali.

Nel Capitolo 13, a conclusione della definizione dei principi e delle regole di condotta adottate dall'Istituto, si è effettuata, a titolo meramente esemplificativo, **una valutazione del rischio di non *compliance* del Modello di Organizzazione, Gestione e Controllo** senza che con ciò si sia inteso determinare una minore attenzione al dettato del D.Lgs 231/2001 e definire situazioni di minore attenzione ai fini del rischio di commissione di reati presupposto 231.

4. PRINCIPI E STANDARD DI CONTROLLO IN RELAZIONE AI REATI CONTRO LA PUBBLICA AMMINISTRAZIONE

Già da un esame sommario risulta evidente che le aree di intervento sistematico dell'Istituto hanno una peculiarità in comune: sono attività che pongono **Isfort in stretto rapporto con la Pubblica Amministrazione** e, **commettere reati in danno della PA** costituisce il primo reato presupposto 231 previsto nella norma (art. 24 del D.Lgs.).

Rinviando alla disamina completa dei reati presupposto 231, così come annotato più dettagliatamente nella Parte Generale del presente modello, si rammenta che tra le fattispecie considerate dalla norma ricadono:

- l'indebita percezione di contributi, finanziamenti o altre erogazioni da parte dello Stato o di altro ente pubblico (art. 316-ter c.p.)
- la truffa in danno dello Stato o di altro ente pubblico (art. 640, 2° comma, n. 1 c.p.);
- la truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.);
- la frode informatica in danno dello Stato o di altro ente pubblico (art. 640-ter c.p.);
- la corruzione per un atto d'ufficio (art. 318 c.p.);
- la corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.);
- la corruzione in atti giudiziari (art. 319-ter c.p.);
- l'istigazione alla corruzione (art. 322 c.p.); la concussione (art. 317 c.p.);
- la malversazione a danno dello Stato o di altro ente pubblico (art. 316- bis c.p.)

A. AREA DEL FARE
4.1. - I responsabili dei centri e delle funzioni che hanno attività di contatto con la Pubblica Amministrazione:
forniscono ai collaboratori direttive sulle modalità di condotta operativa da adottare nei contatti formali e informali intrattenuti con i diversi soggetti pubblici, secondo le deleghe di potere ricevute, trasferendo conoscenza della norma e consapevolezza delle situazioni a rischio reato.
prevedono codici di comportamento in caso di verifiche e ispezioni da parte di soggetti pubblici.
prevedono adeguati meccanismi di tracciabilità circa i flussi informativi verso la PA.
assegnano l'eventuale incarico a soggetti esterni di operare in rappresentanza della società nei confronti della PA in modo formale, prevedendo una specifica clausola che vincoli all'osservanza dei principi etico - comportamentali adottati dalla società.
prescrivono a dipendenti e ai collaboratori di segnalare all'Organismo di Vigilanza ogni violazione o sospetto di violazione del Modello Organizzativo.
prevedono la tutela di dipendenti e collaboratori da ogni conseguenza che possa derivare dalla segnalazione.

assicurano riservatezza dell'identità di chi effettua la segnalazione.
segnalano all'Organismo di Vigilanza i comportamenti a rischio di reato presupposto 231 di cui siano venuti a conoscenza in via diretta o per il tramite di informativa ricevuta dai propri collaboratori.
prescrivono, in misura chiara e ineludibile, i comportamenti di un dipendente o altri collaboratori in caso di tentata concussione da parte di un pubblico funzionario.
forniscono adeguata e tempestiva informativa al proprio dirigente superiore per funzione e all'OdV.
prevedono adeguata protezione del dipendente che ha attivato l'informativa sul tentativo di concussione.
i responsabili dei centri e delle funzioni comunicano tempestivamente all'OdV tutte le notizie apprese ufficialmente, anche da parte da organi di polizia giudiziaria, riguardanti illeciti e/o reati con rischi di impatto aziendale
assicurano adeguata assistenza in caso di contenzioso penale, civile o amministrativo.
Altro

B. AREA DEL NON FARE
4.2. - Con riferimento alle tipologie di reato rilevanti ai sensi del l'art. 24 del D. Lgs. 231/01, sono espressamente vietati, a titolo non esaustivo, i seguenti comportamenti a rischio da evitare nei rapporti con i rappresentanti della PA:
attivare operazioni di natura straordinaria rispetto al profilo soggettivo della committenza o della controparte pubblica
attivare operazioni che prevedano schemi negoziali che possono agevolare l'opacità delle relazioni economiche e finanziarie intercorrenti tra azienda e committenza e/o controparte pubblica
predisporre una articolazione contrattuale opaca e ingiustificata
promettere o effettuare erogazioni in denaro per finalità diverse da quelle istituzionali e di servizio,
promettere o concedere soluzioni di comodo quali, in via non esaustiva, l'erogazione di servizi al di fuori delle modalità standard, interessamento per facilitare l'assunzione di parenti/affini/amici
promettere di fornire o fornire impropriamente, anche tramite terzi, l'erogazione di servizi, omaggi/regalie dirette o indirette non di modico valore
favorire, nei processi d'acquisto, fornitori e sub-fornitori in quanto indicati dai rappresentanti committenza e/o controparte pubblica come condizione per lo svolgimento successivo delle attività o dell'acquisizione di contratto
abusare della posizione di incaricato di pubblico servizio per ottenere utilità a vantaggio della società.
i divieti sopra rappresentati si intendono estesi anche ai rapporti indiretti con i rappresentanti della PA attraverso terzi fiduciari.

altro

4.3. - Inoltre, nei confronti della PA, è fatto divieto di:
tenere una condotta ingannevole che possa indurre la PA in errore nella valutazione tecnico-economica dei servizi offerti
destinare contributi/sovvenzioni/finanziamenti pubblici a finalità diverse da quelle per le quali sono stati ottenuti, o utilizzarli in modalità differenti a quanto previsto dalla normativa di riferimento.
modificare/ omettere/ limitare l'erogazione di tutti gli interventi previsti dalle specifiche convenzioni e relativa contrattualistica.
esibire documenti/dati falsi o alterati per rendicontare le operazioni finanziate con contributi pubblici
omettere informazioni dovute, al fine di orientare a proprio favore le decisioni della PA
accedere in maniera non autorizzata ai sistemi informativi della PA o comunque utilizzati per la rendicontazione alla PA, per ottenere e/o modificare informazioni a vantaggio della società
altro

4.4. – Relativamente alla congruità e al volume delle operazioni è fatto divieto di:
contrattare operazioni incoerenti per ammontare e caratteristiche rispetto al profilo economico e finanziario della committenza
contrattare operazioni non ragionevoli rispetto all'attività svolta dal cliente
contrattare operazioni di frequenza non congrua rispetto all'attività esercitata
proporre o accettare frazionamenti artificiosi dell'ammontare della operazione
contrattare operazioni non congrue rispetto alle finalità dichiarate
contrattare operazioni improvvise e poco giustificate rispetto all'ordinaria attività
contrattare operazioni di ammontare consistente, concentrate in un ristretto arco temporale
contrattare operazioni esorbitanti l'entità delle risorse economiche nella disponibilità del cliente
ricorrere ripetutamente a domiciliazioni di comodo
ricorrere ripetutamente a procure
ricorrere in misura ingiustificata e non congrua a interazioni con aree geografiche a elevato livello di corruzione e di permeabilità con attività criminose
ricorrere in misura ingiustificata e non congrua a interazioni con paesi non dotati di efficaci sistemi di prevenzione del riciclaggio e del finanziamento del terrorismo
altro

5. PRINCIPI E STANDARD DI CONTROLLO IN RELAZIONE AI PROCESSI STRUMENTALI

All'interno delle aree di intervento aziendale, che prevalentemente, ma non in via esclusiva, **si riscontrano orientate verso una committenza pubblica**, l'analisi dei processi strumentali è rivolta a tutte quelle attività aziendali che consentono di generare risorse utili al potenziale compimento dei reati presupposto 231.

Si è compiuta, quindi, una *gap analysis*, basata ancora una volta, principalmente, in relazione a **comportamenti del FARE e del NON FARE,** sulle indicazioni contenute nelle Linee Guida, considerando anche le *best practices* internazionali in tema di rischio di frode e di corruzione.

La *gap analysis* ha individuato come elementi qualificanti **la separazione di ruolo nelle fasi chiave del processo, la tracciabilità degli atti e dei livelli autorizzativi delle singole operazioni**.

Isfort considera i comportamenti e le condotte evidenziate quali elementi qualificanti la propria *policy di governance* e di **efficacia preventiva e garanzia della condizione esimente**, a norma dell'art. 6, comma 1 del 231/2001.

5.1 Finanza dispositiva

Il processo riguarda i flussi monetari e finanziari in uscita con lo scopo di assolvere alle obbligazioni di varia natura contratte dalla società. All'interno del processo si potrebbero costituire disponibilità finanziarie - sia in Italia che all'estero - destinabili al pubblico ufficiale o all'incaricato di pubblico servizio o comunque a terzi per attività illecite. In particolare, gli elementi specifici del FARE sono di seguito rappresentati.

A. AREA DEL FARE
5.1.1. – I processi riguardanti i flussi monetari e finanziari prevedono:
l'esistenza di attori diversi operanti nelle fasi/attività del processo finanziario.
l'esistenza di livelli autorizzativi sia per la richiesta, che per l'ordine di pagamento o di messa a disposizione.
la richiesta dell'ordine di pagamento o di messa a disposizione esclusivamente per iscritto.
la tracciabilità di tutti gli atti e delle singole fasi del processo finanziario.
l'effettuazione del pagamento solo con mezzi tracciabili.
il controllo/riconciliazioni a consuntivo.
eventuali modalità di movimentazioni finanziari non standard sono considerate solo "in deroga" e soggette, pertanto, a criteri di autorizzazione e controllo al più alto livello aziendale.
la comunicazione di flussi monetari e/o finanziari con modalità non standard è obbligatoriamente comunicata all'OdV, per quanto di competenza e con periodicità definita.
Altro

B. AREA DEL NON FARE
5.1.2. - Relativamente ai mezzi di pagamento delle operazioni è fatto divieto di:
precostituire documenti/dati falsi o alterati per il pagamento delle operazioni
omettere informazioni dovute per il pagamento delle operazioni
utilizzare mezzi di pagamento non tracciati
utilizzare conti non propri per trasferire/ricevere fondi
utilizzare valute virtuali
ricorrere ripetutamente a procure e deleghe bancarie
promettere o concedere pagamenti con soluzioni di comodo al di fuori delle modalità standard approvate e di legge
promettere il concambio di servizi come forma di pagamento delle operazioni, anche di modico valore
favorire la scelta di fornitori e sub-fornitori, come forma di pagamento delle operazioni, anche di modico valore
abusare della posizione di incaricato di pubblico servizio per ottenere forme di pagamento al di fuori delle modalità standard approvate e di legge
accedere in maniera non autorizzata ai sistemi informativi interni dell'area finanziaria per effettuare pagamenti e/o modificare informazioni al di fuori delle modalità standard approvate e di legge
i divieti sopra rappresentati si intendono estesi anche ai rapporti indiretti con la committenza attraverso terzi fiduciari
altro

5.2 Selezione e assunzione del personale

La selezione e l'assunzione di personale potrebbero costituire un potenziale supporto alla commissione del reato verso dirigenti della PA o di pubblici servizi che possono agevolare l'opacità delle relazioni economiche e finanziarie.

L'indebito beneficio, ottenuto attraverso l'assunzione di personale, è l'elemento costitutivo del reato presupposto 231, rientranti negli atti del compiere, omettere o ritardare.

A. AREA DEL FARE
5.2.1. – I processi di selezione e assunzione del personale prevedono:
la tracciabilità delle fonti di reperimento dei CV.
una procedura standard di colloquio con i candidati.
modalità trasparenti e standard di valutazione del candidato.

la formulazione della proposta e assunzione sulla base di criteri uniformi di idoneità.
la comunicazione all'OdV dell'elenco delle assunzioni eventualmente effettuate in deroga ai principi sopra elencati.
Altro

B. AREA DEL NON FARE
5.2.2. - Relativamente ai processi riguardanti la selezione e assunzione del personale è fatto divieto di:
precostituire documenti/dati falsi o alterati riguardanti la selezione dei candidati
formulare proposte di assunzione al di fuori delle modalità standard approvate, delle leggi in materia di lavoro di legge e dei CCNL di riferimento ove applicabili
proporre mezzi di pagamento delle prestazioni non tracciabili e per contanti
promettere o concedere pagamenti con soluzioni di comodo al di fuori delle modalità standard approvate e di legge
promettere il concambio di servizi come forma di pagamento delle operazioni, anche di modico valore
favorire la scelta di fornitori e sub-fornitori, come forma di pagamento delle operazioni, anche di modico valore
accedere in maniera non autorizzata ai sistemi informativi interni dell'area risorse umane per operare su situazioni contrattuali e/o modificare informazioni, posizioni retributive e contributive e al di fuori delle modalità standard approvate e di legge
i divieti sopra rappresentati si intendono estesi anche ai rapporti indiretti con i candidati attraverso terzi fiduciari
altro

5.3 Gestione degli omaggi

Il processo di gestione degli omaggi è composto da tutte le attività di distribuzione gratuita di beni e servizi, a clienti, fornitori, lavoratori dipendenti e soggetti estranei alla società, con l'obiettivo di sviluppare l'attività aziendale, creando direttamente la domanda di servizi o promuovendola indirettamente.

La gestione degli omaggi, al di là della normale attività di pubblicità e promozione, attraverso beni e servizi di modico valore potrebbe costituire un potenziale supporto alla commissione del reato verso pubblici dipendenti ed amministratori per ottenerne favori nell'ambito dello svolgimento di altre attività aziendali.

In tale ambito il reato di corruzione è l'indebita percezione, da parte del pubblico ufficiale o dell'incaricato di pubblico servizio, di una qualsiasi utilità per sé o per terzi in conseguenza del compimento, dell'omissione o del differimento di atti dovuti.

A. AREA DEL FARE

5.3.1. – il sistema di controllo del processo di gestione degli omaggi prevede:
la verifica se il destinatario della donazione possa favorire, direttamente o indirettamente, in qualsiasi modo la Società.
l'indicazione, per ciascuna tipologia di servizio, di specifici range economici e relativo importo massimo spendibile.
la separazione di ruolo fra richiedente dell'omaggio e acquirente del bene o servizio.
la definizione di specifiche soglie di valore per gli omaggi destinati a pubblici dipendenti e amministratori.
la registrazione degli omaggi consegnati a pubblici dipendenti e amministratori, la specifica del bene o servizio e il relativo valore.
nel caso di donazioni a enti non profit la verifica della loro regolare costituzione qualora non si tratti di soggetti aventi rilievo nazionale o internazionale.
la conservazione del nominativo dell'ente non profit beneficiario, la tipologia di attività svolta, lo scopo della donazione, i beni o l'entità delle somme, oggetto di donazione.
la comunicazione all'OdV dell'elenco omaggi eventualmente effettuati in deroga ai principi sopra elencati.
Altro

B. AREA DEL NON FARE
5.3.2. - Relativamente alla gestione degli omaggi è fatto divieto di:
promettere o donare beni o denaro se non sussiste per l'azienda un significativo interesse scientifico, artistico, umanitario e/o sociale
effettuare una donazione se non come atto volontario liberale e, senza alcun concambio di un servizio o un beneficio
effettuare una donazione agli enti non profit se non adeguatamente verificati eventualmente con riferimento all'elenco predisposto dall'azienda.
precostituire documenti/dati falsi o alterati per consentire l'erogazione di omaggi al di fuori delle modalità standard approvate e di legge
promettere o effettuare donazioni con soluzioni di comodo al di fuori delle modalità standard approvate e di legge
accedere in maniera non autorizzata ai sistemi informativi interni delle aree coinvolte nel processo di gestione degli omaggi per operare alterare informazioni e/o disposizioni al di fuori delle modalità standard approvate e di legge
i divieti sopra rappresentati si intendono estesi anche al processo di gestione degli omaggi in via indiretta attraverso terzi in particolare attraverso fornitori di beni e servizi usuali
altro

5.4 Spese di rappresentanza

La gestione anomala delle spese di rappresentanza potrebbe costituire un potenziale supporto alla commissione del reato verso pubblici dipendenti ed amministratori per ottenerne favori nell'ambito dello svolgimento di altre attività aziendali.

Il sistema di controllo di Isfort si basa sulla individuazione dei soggetti abilitati a sostenere e ad autorizzare le spese e sulla tracciabilità degli atti.

A. AREA DEL FARE
5.4.1. – il sistema di controllo delle spese di rappresentanza prevede:
l'individuazione delle categorie di spesa effettuabili.
la verifica se il destinatario della spesa possa favorire, direttamente o indirettamente, in qualsiasi modo la Società.
l'indicazione, per ciascuna tipologia di spesa, di specifici range economici e relativo importo massimo spendibile.
l'identificazione dei soggetti aziendali abilitati a sostenere le spese.
la separazione di ruolo fra chi effettua la spesa e chi provvede al rimborso.
la definizione di specifiche soglie di spese di rappresentanza destinate a pubblici dipendenti e amministratori.
la registrazione delle spese di rappresentanza verso pubblici dipendenti e amministratori, la specifica della spesa e il relativo valore.
nel caso di spese di rappresentanza a beneficio di enti non profit la verifica della loro regolare costituzione qualora non si tratti di soggetti aventi rilievo nazionale o internazionale.
la conservazione del nominativo dell'ente non profit beneficiario, la tipologia di attività svolta, lo scopo della spesa e l'entità.
la comunicazione all'OdV delle spese eventualmente effettuate in deroga ai principi sopra elencati.
Altro

B. AREA DEL NON FARE
5.4.2. - Relativamente alla gestione delle spese di rappresentanza è fatto divieto di:
effettuare spese se non sussiste per l'azienda un significativo interesse scientifico, artistico, umanitario e/o sociale
effettuare una spesa se non come atto volontario liberale e, senza alcun concambio di un servizio o un beneficio

effettuare una spesa a favore di enti non profit se non adeguatamente verificati eventualmente con riferimento all'elenco predisposto dall'azienda.
precostituire documenti/dati falsi o alterati per consentire spese di rappresentanza al di fuori delle modalità standard approvate e di legge
promettere o effettuare spese di rappresentanza con soluzioni di comodo al di fuori delle modalità standard approvate e di legge
accedere in maniera non autorizzata ai sistemi informativi interni delle aree coinvolte nel processo di gestione delle spese di rappresentanza per operare alterare informazioni e/o disposizioni al di fuori delle modalità standard approvate e di legge
i divieti sopra rappresentati si intendono estesi anche al processo di spese di rappresentanza in via indiretta attraverso terzi in particolare attraverso fornitori di beni e servizi usuali
altro

5.5 Consulenze e prestazioni professionali

Il conferimento di incarichi di consulenza e prestazioni professionali è un processo aziendale che necessita di estrema attenzione in quanto in esso possono realizzarsi condotte illecite (omettere, ritardare etc) attraverso l'assegnazione di incarichi non trasparenti quali per esempio:

- la contrattualizzazione con terzi per servizi a prezzi superiori a quelli di mercato col fine di creare riserve di fondi
- l'assegnazione di incarichi a persone o società gradite a pubblici ufficiali o incaricati di pubblico servizio per ottenerne favori nell'ambito dello svolgimento di altre attività aziendali

A. AREA DEL FARE
5.5.1. – Su queste basi in Isfort il sistema di controllo degli incarichi di consulenza e prestazioni professionali prevede:
l'individuazione delle categorie di incarichi conferibili.
la verifica degli attori diversi operanti nelle fasi/attività del processo anche con riferimento al Manuale della Qualità.
l'identificazione dei soggetti aziendali abilitati a proporre l'incarico.
l'indicazione, per ciascuna tipologia di incarico, di specifici range economici e relativo importo massimo spendibile.
la verifica dei requisiti professionali, economici ed organizzativi del destinatario dell'incarico a garanzia degli standard qualitativi richiesti dal Manuale della Qualità.
la verifica se il destinatario dell'incarico possa favorire, direttamente o indirettamente, in qualsiasi modo la Società.

la verifica della congruità dell'incarico rispetto a budget approvati.
la valutazione della congruità dell'incarico al di fuori di budget approvati, delle modalità standard approvate.
la definizione dei limiti spesa in relazione alle deleghe.
la separazione di ruolo fra chi formula la richiesta di consulenza, chi la autorizza, chi valida la prestazione resa, chi propone l'eventuale non conformità e chi dispone il pagamento.
la creazione di un registro degli incarichi con la specifica se a budget o fuori budget, la specifica della spesa e il relativo valore.
la tracciabilità delle singole fasi del processo per consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte.
nel caso di incarichi conferiti a enti non profit la verifica della loro regolare costituzione qualora non si tratti di soggetti aventi rilievo nazionale o internazionale.
la conservazione del nominativo dell'ente non profit beneficiario, la tipologia di attività svolta, lo scopo della spesa e l'entità.
la comunicazione all'OdV, con periodicità definita, il preventivo ed il consuntivo delle attività di consulenza / prestazioni professionali suddivise per fornitore.
la comunicazione all'OdV degli incarichi eventualmente conferiti in deroga ai principi sopra elencati.
Altro

B. AREA DEL NON FARE
5.5.2. - Relativamente al conferimento di incarichi di consulenza e prestazioni professionali è fatto divieto di:
proporre o conferire incarichi se non sussiste per l'azienda una significativa necessità produttiva legata all'attività propria dell'azienda e ai processi identificati dal Manuale di Qualità
proporre o conferire incarichi che possano prefigurare concambio di un servizio o un beneficio.
proporre o conferire incarichi se non è stata espletata adeguata attività selettiva fra diversi offerenti e di obiettiva comparazione delle offerte in base a criteri oggettivi e documentabili
conferire incarichi utilizzando dispositivi contrattuali non approvati dall'azienda o non adeguatamente formalizzati
conferire incarichi a enti non profit se non adeguatamente verificati eventualmente con riferimento all'elenco predisposto dall'azienda
precostituire documenti/dati falsi o alterati per consentire il conferimento di incarichi al di fuori delle modalità standard approvate e di legge
promettere o conferire incarichi con soluzioni di comodo al di fuori delle modalità standard approvate e di legge
accedere in maniera non autorizzata ai sistemi informativi interni delle aree coinvolte nel processo di conferimento degli incarichi per operare alterare informazioni e/o disposizioni al di fuori delle modalità standard approvate e di legge

i divieti sopra rappresentati si intendono estesi anche al processo di conferimento di incarichi in via indiretta attraverso terzi in particolare attraverso fornitori di beni e servizi usuali
altro

5.6 Acquisti di beni e servizi

L'acquisto di beni e servizi è un processo aziendale che, analogamente al conferimento di incarichi di consulenza, deve essere sottoposto a continui controllo in quanto in esso possono realizzarsi condotte illecite per esempio attraverso:

- la contrattualizzazione con fornitori a prezzi superiori a quelli di mercato col fine di creare riserve di fondi
- l'acquisto da fornitori graditi a pubblici ufficiali o incaricati di pubblico servizio per ottenerne favori nell'ambito dello svolgimento di altre attività aziendali

Come in altri processi il sistema di controllo si basa sulla formalizzata separazione di ruolo nelle fasi chiave del processo, della tracciabilità degli atti e della valutazione complessiva delle forniture.

A. AREA DEL FARE
5.6.1. – Su queste basi in Isfort il sistema di controllo degli acquisti di beni e servizi prevede:
la verifica degli attori diversi operanti nelle fasi/attività del processo anche con riferimento al Manuale della Qualità.
l'identificazione dei soggetti aziendali abilitati a proporre l'acquisto.
la definizione di criteri tecnico-economici per la selezione di potenziali fornitori.
l'adeguata comparazione delle offerte sulla base di criteri oggettivi e documentabili.
la verifica dei requisiti professionali, economici ed organizzativi del fornitore a garanzia degli standard qualitativi richiesti dal Manuale della Qualità.
la verifica se il fornitore possa favorire, direttamente o indirettamente, in qualsiasi modo la Società.
la verifica della congruità della fornitura, in particolare di servizi, rispetto a budget approvati.
la valutazione della congruità della fornitura al di fuori di budget approvati, delle modalità standard approvate.
la definizione dei limiti spesa in relazione alle deleghe.
la separazione di ruolo fra chi formula la richiesta di acquisto, chi la autorizza, chi valida la prestazione resa, chi propone l'eventuale non conformità e chi dispone il pagamento.
la creazione di un registro delle forniture, non di modico valore, con la specifica se a budget o fuori budget, la specifica della spesa e il relativo valore.

la tracciabilità delle singole fasi del processo di acquisto per consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte.
nel caso di acquisti da enti non profit la verifica della loro regolare costituzione qualora non si tratti di soggetti aventi rilievo nazionale o internazionale.
la conservazione del nominativo dell'ente non profit beneficiario, la tipologia di attività svolta, lo scopo della spesa e l'entità.
la comunicazione all'OdV, con periodicità definita, il preventivo ed il consuntivo degli acquisti non di modico valore suddivise per fornitore.
la comunicazione all'OdV degli acquisti eventualmente conferiti in deroga ai principi sopra elencati.
Altro

B. AREA DEL NON FARE
5.6.2. - Relativamente agli acquisti di beni e servizi è fatto divieto di:
proporre o effettuare acquisti se non sussiste per l'azienda una significativa necessità produttiva legata all'attività propria dell'azienda e ai processi identificati dal Manuale di Qualità
proporre o effettuare acquisti che possano prefigurare concambio di un servizio o un beneficio.
proporre o effettuare acquisti se non è stata espletata adeguata attività selettiva fra diversi fornitori e di obiettiva comparazione delle offerte in base a criteri oggettivi e documentabili
effettuare acquisti utilizzando dispositivi contrattuali non approvati dall'azienda o non adeguatamente formalizzati
effettuare acquisti da enti non profit se non adeguatamente verificati eventualmente con riferimento all'elenco predisposto dall'azienda
precostituire documenti/dati falsi o alterati per consentire acquisti al di fuori delle modalità standard approvate e di legge
promettere o effettuare acquisti con soluzioni di comodo al di fuori delle modalità standard approvate e di legge
accedere in maniera non autorizzata ai sistemi informativi interni delle aree coinvolte nel processo di acquisti di beni e servizi per operare alterare informazioni e/o disposizioni al di fuori delle modalità standard approvate e di legge
i divieti sopra rappresentati si intendono estesi anche al processo di acquisti in via indiretta attraverso terzi in particolare attraverso fornitori di beni e servizi usuali
altro

5.7 Sponsorizzazioni

Una gestione opaca e anomala delle sponsorizzazioni può evidentemente costituire una opportunità di creazione di fondi per ottenere favori nell'ambito dello svolgimento di altre attività aziendali.

In linea di principio i contratti di sponsorizzazione devono obbligare la società a contributi, prestazioni di servizi e/o fornitura di beni nei confronti di un soggetto solo se:

- è evidente il ritorno di immagine e la finalità di promozione della società
- sono definiti i criteri per l'individuazione dei progetti di sponsorizzazione
- se è presente una idonea strutturazione contrattuale

A. AREA DEL FARE
5.7.1. – Su queste basi in Isfort il sistema di controllo delle sponsorizzazioni prevede:
la verifica degli attori diversi operanti nelle fasi/attività del processo anche con riferimento al Manuale della Qualità.
l'identificazione dei soggetti aziendali abilitati a proporre una sponsorizzazione.
la verifica di un interesse reale e concreto e di un adeguato ritorno di immagine per l'azienda.
l'oggetto del contratto di sponsorizzazione è determinato e sono individuate in maniera specifica, le attività connesse alla sponsorizzazione.
la verifica della congruità tra contributo versato per la sponsorizzazione e la controprestazione promozionale ricevuta in base ai prezzi di mercato.
la verifica dei requisiti professionali, economici ed organizzativi di chi effettua la controprestazione promozionale a garanzia degli standard qualitativi richiesti dal Manuale della Qualità.
la verifica se la sponsorizzazione possa favorire, direttamente o indirettamente, in qualsiasi modo la Società.
la verifica della congruità della sponsorizzazione rispetto a budget approvati.
la valutazione della congruità della sponsorizzazione al di fuori di budget approvati, delle modalità standard approvate.
la definizione dei limiti spesa in relazione alle deleghe.
la separazione di ruolo fra chi, a livello aziendale, propone la sponsorizzazione, chi la autorizza, chi valida il ritorno aziendale, chi propone l'eventuale non conformità e chi dispone il pagamento.
la creazione di un registro delle sponsorizzazioni, non di modico valore, con la specifica se a budget o fuori budget, la specifica della spesa e il relativo valore.
la tracciabilità delle singole fasi del processo di sponsorizzazione per consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte.
nel caso di sponsorizzazione a enti non profit la verifica della loro regolare costituzione qualora non si tratti di soggetti aventi rilievo nazionale o internazionale.
la conservazione del nominativo dell'ente non profit beneficiario, la tipologia di attività svolta, lo scopo della spesa e l'entità.
la comunicazione all'OdV, con periodicità definita, il preventivo ed il consuntivo delle sponsorizzazioni non di modico valore suddivise per fornitore.

la comunicazione all'OdV delle sponsorizzazioni eventualmente effettuate in deroga ai principi sopra elencati.
Altro

B. AREA DEL NON FARE
5.7.2. - Relativamente alle sponsorizzazioni è fatto divieto di:
proporre o effettuare sponsorizzazioni se non sussiste per l'azienda una congruità legata all'attività propria dell'azienda e ai processi identificati dal Manuale di Qualità
proporre o effettuare sponsorizzazioni che possano prefigurare concambio di un servizio o un beneficio indiretto non legato a un ritorno di immagine
proporre o effettuare sponsorizzazioni se non è stata espletata adeguata attività selettiva fra le potenziali proposte e una obiettiva comparazione delle proposte in base a criteri oggettivi e documentabili
effettuare sponsorizzazioni utilizzando dispositivi contrattuali non approvati dall'azienda o non adeguatamente formalizzati
effettuare sponsorizzazioni a enti non profit se non adeguatamente verificati eventualmente con riferimento all'elenco predisposto dall'azienda
precostituire documenti/dati falsi o alterati per consentire acquisti al di fuori delle modalità standard approvate e di legge
promettere o effettuare sponsorizzazioni con soluzioni di comodo al di fuori delle modalità standard approvate e di legge
accedere in maniera non autorizzata ai sistemi informativi interni delle aree coinvolte nel processo di promozione dell'azienda per operare alterare informazioni e/o disposizioni al di fuori delle modalità standard approvate e di legge
i divieti sopra rappresentati si intendono estesi anche al processo di sponsorizzazione in via indiretta attraverso terzi in particolare attraverso fornitori di beni e servizi usuali
altro

6. PRINCIPI E STANDARD DI CONTROLLO IN RELAZIONE AI REATI SOCIETARI

I reati societari attengono in linea di principio alla conduzione dell'azienda da parte dell'Organo amministrativo e di altri dallo stesso delegati e di principio si concretizzano in un **danno patrimoniale nei confronti dei soci e di altri stakeholders ovvero nella fattispecie di azioni lesive del mercato e dei risparmiatori**.

In massima parte il **soggetto attivo del reato è l'Organo amministrativo**, anche se è ipotizzabile il coinvolgimento, a titolo di concorso, dei soci, di sindaci, liquidatori, altri soggetti apicali, dipendenti e collaboratori coinvolti nelle operazioni ovvero che esercitano in misura continuativa poteri oltre a terzi beneficiari dell'operazione.

Il sistema di controllo di Isfort si basa sulla **individuazione dei soggetti abilitati** a determinare la commissione dei reati e sulla tracciabilità degli atti.

In relazione ai reati e alle condotte criminose collegate, descritti più avanti, i processi aziendali più specificamente coinvolti sono:

- la gestione della contabilità generale, sia in sede di imputazione delle scritture contabili, sia in sede di verifica dei dati contabilizzati
- la predisposizione del bilancio di esercizio, nonché delle situazioni patrimoniali redatte per specifiche necessità, soprattutto se di natura valutativa o stimata
- la gestione delle operazioni bancarie e finanziarie
- la predisposizione di relazioni accompagnatorie, soprattutto se di operazioni di finanza straordinaria
- la gestione del capitale sociale, soprattutto se in sede di effettuazione di operazioni di finanza straordinaria o di liquidazione, degli utili e delle riserve
- la gestione dei rapporti con i Soci ed il Collegio Sindacale in sede di verifica delle situazioni amministrative, finanziarie, fiscali e contabili
- la gestione delle attività connesse al funzionamento dell'assemblea dei Soci
- il compimento di operazioni rilevanti o straordinarie con soggetti terzi
- la gestione della sicurezza dei dati informatici.

Si elencano di seguito i reati societari presupposto 231, con il riferimento ai relativi articoli del Codice civile, e successivamente si descrive il monitoraggio dei comportamenti del FARE e del NON FARE:

6.1 Falsità in comunicazioni, prospetti e relazioni

• False comunicazioni sociali in danno della società, dei soci o dei creditori (artt. 2621 e 2622 c.c.).

6.2 Tutela penale del capitale sociale

• Indebita restituzione dei conferimenti (art. 2626 c.c.).

• Illegale ripartizione degli utili o delle riserve (art. 2627 c.c.)

• Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.).

• Operazioni in pregiudizio dei creditori (art. 2629 c.c.)

• Formazione fittizia del capitale (art. 2632 c.c.)

• Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.)

In questo caso soggetti attivi del reato sono i liquidatori.

6.3 Tutela penale del regolare funzionamento degli organi sociali

• Impedito controllo (art. 2625 c.c.)

• Illecita influenza sull'assemblea (art. 2636 c.c.)

6.4. Tutela penale contro le frodi

• Aggiotaggio (art. 2637 c.c.)

Soggetto attivo del reato può essere chiunque, anche estraneo alla società, ma riveste interesse ai sensi del reato presupposto 231 il coinvolgimento degli amministratori.

A. AREA DEL FARE
6.4.1 – Su queste basi in Isfort il sistema di controllo in relazione ai reati societari prevede:
il rispetto delle norme di legge e delle procedure aziendali in tutte le attività finalizzate alla formazione del bilancio, di situazioni contabili redatte in occasione di eventi specifici e delle altre comunicazioni sociali.
la definizione di procedure aziendali volte a preservare l'integrità del capitale sociale, nel rispetto delle norme di legge, al fine di non ledere le garanzie dei creditori e dei terzi in genere.
la verifica degli attori diversi operanti nelle fasi/attività del processo anche con riferimento ai poteri conferiti.
la verifica periodica del funzionamento della società e degli organi sociali.
la verifica delle forme di controllo interno sulla gestione sociale previsto dalla legge.
la libera e corretta formazione della volontà assembleare.
una normativa interna che assicura il rispetto dei criteri di correttezza sostanziale e procedurale nel compimento di operazioni societarie significative, soprattutto se straordinarie, concluse sia con soggetti terzi sia con parti correlate.
la verifica periodica della coerenza e validità di deleghe di poteri aziendali in materia societaria.
l'informazione ai soci ed al pubblico in generale appropriata sulla situazione economica, patrimoniale e finanziaria della Società;
l'emanazione, da parte dell'OdV, di istruzioni relative ai comportamenti da seguire nell'ambito delle aree a rischio, in relazione ai reati societari.

l'esame, da parte dell'OdV, di eventuali segnalazioni specifiche provenienti dagli organi di controllo, da terzi o da qualsiasi esponente aziendale ed effettuazione degli accertamenti ritenuti necessari od opportuni in conseguenza delle segnalazioni ricevute.
la vigilanza sull'effettiva sussistenza delle condizioni per garantire ai sindaci una concreta autonomia nelle rispettive funzioni di controllo delle attività aziendali.
la comunicazione all'OdV delle deroghe ai principi sopra elencati.
Altro

B. AREA DEL NON FARE
6.4.2. - Relativamente in relazione ai reati societari è fatto divieto di:
omettere di comunicare dati ed informazioni imposti dalla normativa e dalle procedure in vigore riguardo alla situazione economica, patrimoniale e finanziaria della Società
predisporre, rappresentare o comunicare dati falsi, lacunosi o comunque suscettibili di fornire una descrizione non rispondente alla realtà, riguardo alla situazione economica, patrimoniale e finanziaria della Società
disattendere i principi, le norme e le procedure aziendali in materia di redazione di bilanci, relazioni ed informativa
effettuare comunicazioni diverse dalla informativa contabile periodica rivolte ai soci, ai creditori o al pubblico in generale riguardo alla situazione economica, patrimoniale e finanziaria della Società
restituire conferimenti ai soci o liberare gli stessi dall'obbligo di eseguirli, al di fuori dei casi di legittima riduzione del capitale sociale
ripartire utili non effettivamente conseguiti o destinati per legge a riserva, nonché ripartire riserve che non possono per legge essere distribuite
acquistare o sottoscrivere azioni della Società fuori dai casi previsti dalla legge
procedere in ogni modo a formazione o aumento fittizi del capitale sociale, attribuendo azioni per un valore inferiore a quello nominale in sede di aumento del capitale sociale
distrarre o ripartire i beni sociali tra i soci – in fase di liquidazione – prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessarie per soddisfarli
effettuare riduzioni del capitale sociale, fusioni o scissioni in violazione delle disposizioni di legge a tutela dei creditori
porre in essere comportamenti che impediscano materialmente, o che comunque ostacolino, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, lo svolgimento dell'attività di controllo o di revisione della gestione sociale da parte del Collegio Sindacale o dei soci
determinare o influenzare le deliberazioni dell'assemblea, mediante atti simulati o fraudolenti volti ad alterare la regolare formazione della volontà assembleare.
predisporre e divulgare dati o notizie comunque relativi alla Società salvo autorizzazioni aziendali specifiche
accedere in maniera non autorizzata ai sistemi informativi interni delle aree coinvolte nel processo di gestione societaria dell'azienda per operare alterare informazioni e/o disposizioni al di fuori delle modalità standard approvate e delle norme di legge

i divieti sopra rappresentati si intendono estesi anche al processo di gestione societaria dell'azienda in via indiretta attraverso operazioni concertate con terzi
altro

7. PRINCIPI E STANDARD DI CONTROLLO IN RELAZIONE AI REATI DI RICICLAGGIO E RICETTAZIONE

La commissione dei reati contemplati dall'art. 25 octies del D.Lgs 231/2008, ovvero la ricettazione, il riciclaggio e l'impiego di denaro, beni o utilità di provenienza illecita, nonché l'autoriciclaggio, attraverso l'impiego a qualsiasi titolo di denaro contante, libretti di deposito o titoli al portatore (quali libretti bancari e postali, assegni, vaglia, certificati di deposito) in misura pari o superiore a Euro …… appare, in linea di principio, in ambito Isfort, una ipotesi difficilmente realizzabile.

In questa fattispecie di reati, in massima parte, sono **soggetti attivi** le posizioni apicali aziendali, dotate di deleghe, ma possono vedere frequentemente coinvolti nelle operazioni dipendenti e collaboratori principalmente nei seguenti processi aziendali:

- gestione dei rapporti con Clienti (non PA), Fornitori e Partner
- gestione dei flussi finanziari in entrata ed in uscita
- gestione dei rimborsi e spese di rappresentanza

B. AREA DEL FARE
7.1. – Su queste basi in Isfort il sistema di controllo dei reati di riciclaggio e ricettazione (art. 25 octies) prevede:
la verifica dell'attendibilità commerciale e professionale dei clienti, dei fornitori e dei partner societari, commerciali e finanziari.
la verifica che tali soggetti non abbiano sede o residenza ovvero qualsiasi collegamento con paesi considerati come non cooperativi in base alle norme contro il riciclaggio di denaro.
la verifica che tali soggetti non siano noti o sospettati, su base documentata di legami con organizzazioni criminali o terroristiche.
l'effettuazione di controlli formali e sostanziali dei flussi finanziari aziendali ripetuti e casuali.
l'effettuazione di controlli formali e sostanziali degli Istituti di credito utilizzati nel compimento delle operazioni, sia scelti dalla società sia indicati dai soggetti con cui l'azienda mantiene rapporti finanziari.
la verifica degli eventuali schermi societari e/o strutture fiduciarie utilizzate nel compimento di operazioni straordinarie.
la verifica di eventuali segnalazioni specifiche provenienti da qualsiasi fonte ed effettuare gli accertamenti ritenuti necessari od opportuni in conseguenza delle segnalazioni ricevute.
l'identificazione dei soggetti aziendali abilitati a proporre una operazione finanziaria o a poter disporre operazioni di cassa e bancarie.
la verifica della congruità delle operazioni di cassa e bancarie rispetto a budget approvati.
l'oggetto delle operazioni finanziarie è determinato e sono individuate in maniera specifica, le prestazioni connesse.
la definizione dei limiti spesa in relazione alle deleghe.

la creazione di un registro delle sponsorizzazioni, non di modico valore, con la specifica se a budget o fuori budget, la specifica della spesa e il relativo valore.
la tracciabilità delle singole fasi del processo finanziario e di cassa per consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte.
la comunicazione all'OdV, con periodicità definita, delle operazioni finanziarie non di modico valore suddivise per soggetti con cui l'azienda mantiene rapporti finanziari.
la comunicazione all'OdV delle operazioni eventualmente effettuate in deroga ai principi sopra elencati.
Altro

B. AREA DEL NON FARE
7.2. - Relativamente ai reati di riciclaggio e ricettazione (art. 25 octies) è fatto divieto di:
proporre o effettuare operazioni finanziarie se non sussiste per l'azienda una corrispondenza alle norme di legge, una congruità legata all'attività propria dell'azienda, e ai processi identificati dal Manuale di Qualità
proporre o effettuare operazioni finanziarie che possano prefigurare concambio di un servizio o un beneficio indiretto
accettare o utilizzare strumenti finanziari o mezzi di pagamento al portatore, diversi da quelli che transitano sui normali canali bancari
accettare denaro e titoli al portatore per importi eccedenti Euro 2.000 per singola operazione, se non tramite intermediari abilitati
effettuare ripetute operazioni di cassa in entrata e in uscita, oltre l'operatività ordinaria, col fine di superare i limiti di legge
proporre o effettuare operazioni finanziarie se non è stata espletata adeguata attività selettiva dell'attendibilità commerciale e professionale dei clienti, dei fornitori e dei partner societari, commerciali e finanziari in base a criteri oggettivi e documentabili
effettuare operazioni finanziarie utilizzando dispositivi contrattuali non approvati dall'azienda o non adeguatamente formalizzati
precostituire documenti/dati falsi o alterati per consentire/ effettuare operazioni finanziarie al di fuori delle modalità aziendali approvate e di legge
promettere o effettuare operazioni finanziarie con soluzioni di comodo al di fuori delle modalità aziendali approvate e di legge
accedere in maniera non autorizzata ai sistemi informativi interni delle aree coinvolte nel processo finanziario dell'azienda per operare alterare informazioni e/o disposizioni al di fuori delle modalità standard approvate e di legge
avere rapporti, nel contesto aziendale, con persone o entità che possano compromettere in alcun modo l'integrità, la reputazione e l'immagine della società
avere un comportamento non collaborativo con le Autorità di Polizia in sede ispettiva o con le Autorità Giudiziarie
i divieti sopra rappresentati si intendono estesi anche a operazioni finanziarie effettuate in via indiretta attraverso operazioni concertate con terzi
altro

8. PRINCIPI E STANDARD DI CONTROLLO IN RELAZIONE AI REATI IN MATERIA DI SICUREZZA SUL LAVORO

I riferimenti normativi della fattispecie di reato considerata, sono gli obblighi dettati dal D.Lgs 81/2008 (il Testo Unico in materia di tutela della salute e della sicurezza nei luoghi di lavoro) che determinano l'inserimento nell'art. 25 septies del D.lgs.231/2008, dei reati quali le lesioni colpose gravi e gravissime e l'omicidio colposo derivanti dalla violazione di norme antinfortunistiche e di tutela di igiene e salute sul luogo di lavoro.

La commissione dei reati contemplati dal citato art. 25 septies del D.Lgs 231/2008 potrebbe apparire, in linea di principio, una ipotesi difficilmente realizzabile in ambito Isfort in quanto in azienda si svolgono principalmente attività di ufficio non legate a lavorazioni rischiose, ma eventi interni all'azienda, anche casuali, o imprevedibili quali l'emergenza Covid 19, determinano un rafforzamento di attenzione sulla materia.

Non a caso Isfort ha provveduto sollecitamente ad **adeguare il proprio DVR** ai rischi Covid 19 e alle norme di legge collegate, redigendo il **Documento di valutazione e gestione del rischio biologico potenziale e non intenzionale da Corona Virus negli ambienti di lavoro**.

In questa fattispecie di reati, in massima parte, sono **soggetti attivi** le posizioni apicali aziendali, dotate di deleghe, ma possono vedere frequentemente coinvolti nelle operazioni dipendenti e collaboratori principalmente nelle situazioni di negligenza, imperizia e mancata osservanza delle prescrizioni di legge e aziendali.

C. AREA DEL FARE
8.1. – Su queste basi in Isfort il sistema di controllo dei reati in materia di sicurezza sul lavoro (art. 25 septies) prevede:
il rispetto degli standard tecnico-strutturali di legge relativi alle attrezzature, agli impianti, ai luoghi di lavoro.
la valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione.
la predisposizione, approvazione, comunicazione e gestione continuativa del DVR e delle deleghe operative conseguenti al personale preposto per legge (in particolare del RSPP).
l'acquisizione di documentazioni e certificazioni obbligatorie di legge.
la conseguente adozione di conseguenti misure inerenti alle attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza.
la predisposizione delle attività di sorveglianza sanitaria di legge, incluso il medico competente.
la tutela dei lavoratori maggiormente a rischio (lavoratori con disabilità, stranieri, donne in gravidanza, madri che allattano) e conseguente valutazione dei percorsi interni e della posizione delle strutture e degli accessi

la programmazione e il costante controllo degli interventi manutentivi di attrezzature, impianti e infrastrutture e di pulizia coerentemente con il piano di manutenzione previsto nel DVR.
la valutazione dello stress lavoro-collegato in relazione alle condizioni aziendali (eventi sentinella quali turnover, assenze, percentuali incidenti e malattie, segnalazioni del medico competente, sanzioni, segnalazione del personale)
la predisposizione delle attività di informazione e formazione dei lavoratori; riguardanti le attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori.
la consultazione periodica dei rappresentanti dei lavoratori per la sicurezza (RLS) secondo la normativa vigente;
l'espresso obbligo per le posizioni apicali aziendali, dipendenti, in via diretta, e collaboratori esterni, al rispetto delle prescrizioni di legge e aziendali, tramite apposite clausole contrattuali.
la verifica periodica dell'applicazione e dell'efficacia delle procedure adottate.
l'effettuazione di controlli formali e sostanziali delle misure di prevenzione e protezione ripetuti e casuali.
l'effettuazione periodica della manutenzione dei sistemi di prevenzione e protezione antincendio.
la verifica di eventuali segnalazioni specifiche provenienti da qualsiasi fonte e l'effettuazione degli accertamenti ritenuti necessari od opportuni in conseguenza delle segnalazioni ricevute.
la tracciabilità delle singole fasi del processo di prevenzione e protezione per consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte.
la comunicazione all'OdV, con periodicità definita, delle operazioni di prevenzione e protezione.
la comunicazione all'OdV delle operazioni eventualmente effettuate in deroga ai principi sopra elencati.
Altro

B. AREA DEL NON FARE
8.2. - Relativamente ai reati dei reati in materia di sicurezza sul lavoro (art. 25 septies) è fatto divieto per tutti, posizioni apicali, dipendenti e collaboratori di:
porre in essere comportamenti in violazione delle prescrizioni di legge e aziendali in materia di tutela della salute e della sicurezza nei luoghi di lavoro
porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato in materia di tutela della salute e della sicurezza nei luoghi di lavoro, possano essere potenzialmente rischiose.
effettuare interventi manutentivi e di pulizia non coerenti con il piano di manutenzione o di iniziativa personale

eseguire interventi sugli impianti e attrezzature senza autorizzazione dell'azienda o senza le idonee protezioni e cautele
utilizzare in maniera impropria o al di fuori delle condizioni di normale uso computer, video terminali e altre attrezzature elettroniche intervenendo su esse con iniziative personali
utilizzare in maniera impropria o al di fuori delle condizioni di normale uso attrezzature d'ufficio o complementi di arredo
procedere a movimentazione di materiale di ufficio e faldoni di documenti di peso cospicuo all'interno degli uffici o nei locali di archivio senza le idonee protezioni, attrezzature e cautele
archiviare materiale di ufficio o faldoni di documenti senza considerarne il peso in relazione al luogo o alle strutture di stoccaggio
conservare negli uffici o nei locali di archivio, inclusa cantina, sostanze combustibili, esplosive, velenose, in ogni caso pericolose senza autorizzazione dell'azienda
intervenire, se non adeguatamente abilitati e protetti, sul quadro elettrico, sulle reti elettriche, di illuminazione, di riscaldamento, di climatizzazione al di fuori della ordinaria regolazione
utilizzare in misura impropria i presidi antincendio, intervenendo in caso di necessità solo se adeguatamente formati in qualità di personale addetto alla gestione emergenza, in grado di attivare le prime misure di intervento, di assicurare l'evacuazione del personale e la chiamata dei soccorsi
intervenire in caso di emergenza sanitaria solo se adeguatamente formati in qualità di personale di primo soccorso, in grado di riconoscere l'emergenza e allertare il sistema di soccorso
posizionare arredi, depositare rifiuti o materiale ingombrante in prossimità delle vie di fuga
precostituire documenti/dati falsi o alterati per consentire/ effettuare operazioni in materia di sicurezza sul lavoro al di fuori delle modalità aziendali approvate e di legge
accedere in maniera non autorizzata ai sistemi informativi interni delle aree coinvolte nel processo di sicurezza sul lavoro per operare alterare informazioni e/o disposizioni al di fuori delle modalità standard approvate e di legge
avere un comportamento non collaborativo con le Autorità competenti in sede ispettiva o con le Autorità Giudiziarie
i divieti sopra rappresentati si intendono estesi anche a operazioni in materia di sicurezza sul lavoro effettuate in via indiretta attraverso operazioni concertate con terzi
altro

9. PRINCIPI E STANDARD DI CONTROLLO IN RELAZIONE AI REATI INFORMATICI

I riferimenti normativi delle fattispecie di reato considerate (art. 24 bis) sono obblighi dettati dalle modifiche introdotte nel Codice penale a seguito del recepimento nell'ordinamento italiano delle **norme europee sulla criminalità informatica** (L. 48 del 18 marzo 2008).

Merita rammentare che le conseguenti modifiche in materia, apportate al Codice penale, puniscono, con gravi pesanti sanzioni e condanne, chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici.

Il contenuto delle predette prescrizioni sembra attenere a realtà operative criminose e del tutto estranee a Isfort tuttavia mentre sono relativamente conosciuti i rischi dovuti alle minacce telematiche generate dai soggetti esterni all'impresa, che attraverso programmi e false comunicazioni cercano di danneggiare i sistemi informatici o di acquisire informazioni utili per successive truffe o frodi, sono spesso sottovalutati i rischi legati ai comportamenti degli agenti interni all'organizzazione (dipendenti, consulenti, fornitori) che, per mezzo di un uso inappropriato di reti, computer aziendali e programmi SW, possono esporre l'impresa a responsabilità dirette e generare danni verso terzi.

Si annota, altresì, che i sistemi informatici e telematici aziendali, le informazioni, i dati o i programmi in essi contenuti sono strettamente coinvolti nel **trattamento dei dati personali di personale e terzi** comunque collegati all'azienda.

Conseguentemente Isfort ha effettuato tutti gli **adempimenti in materia di privacy, a norma del recente Regolamento UE 679/2016**, effettuando il monitoraggio delle risorse HW e SW utilizzate in aree aziendali ed elaborando tutte le misure tecniche ed organizzative necessarie a ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati trattati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità per le quali i dati sono stati raccolti fino alle violazioni intenzionali dei dati personali (*data breach*).

Nella commissione di reati informatici, in massima parte, sono **soggetti attivi** le posizioni apicali aziendali, dotate di deleghe, il personale dei servizi informatici, ma sono frequentemente coinvolti dipendenti, collaboratori e fornitori principalmente per situazioni di negligenza, imperizia e mancata osservanza delle prescrizioni di legge e aziendali.

Isfort mette a disposizione dei citati soggetti attivi una dotazione informatica costituita, secondo le diverse esigenze degli utilizzatori nello svolgimento delle attività loro affidate, da personal computer, notebook, tablet, stampanti, penne ottiche, software, accessori informatici, servizi di accesso alla rete e alla posta elettronica cumulativamente o distintamente tra loro.

D. AREA DEL FARE
9.1. – Su queste basi in Isfort il sistema di controllo dei reati informatici (art. 24 bis) prevede:

l'installazione di dotazioni HW e SW in ambito aziendale unicamente da personale dei servizi informatici e/o tecnici esterni, comunque autorizzati dalla società.
il rispetto degli standard tecnico-strutturali di legge relativi alle attrezzature informatiche, alle reti, ai server, all'HW e SW installati nei luoghi di lavoro.
l'installazione di adeguati sistemi di controllo dei log di accesso, di firewall e filtri di protezione e di backup dei dati.
la registrazione, su archivi informatici, dei livelli di autorizzazione all'accesso (alla rete aziendale e/o a sistemi di proprietà di terzi) da parte degli utenti, ai fini della tracciabilità degli accessi e delle attività informatiche poste in essere per consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte.
la formazione e preparazione specifica del personale dei servizi informatici.
la programmazione e il costante controllo degli interventi manutentivi di attrezzature informatiche coerentemente con il piano di manutenzione previsto nel DVR.
un protocollo di custodia delle password di accesso alla rete aziendale ed alle diverse applicazioni e delle chiavi personali secondo criteri idonei a impedirne una facile individuazione ed un uso improprio.
la previsione di modifica di password, con cadenza predefinita e depositate in azienda in busta chiusa ed in locale protetto
l'accesso ai server (fisico o per via remota) esclusivamente a persone autorizzate.
la stipula di contratti di acquisto di HW e SW o di incarichi relativi ad uno o più processi del sistema informatico (sviluppo di software, utilizzo di applicazioni, anche di rete, manutenzioni, etc.) solo a fornitori di attendibilità commerciale e professionale verificata.
l'acquisizione dai fornitori della documentazione e certificazioni obbligatorie di legge o funzionali all'efficienza del sistema informatico.
un protocollo di utilizzo delle caselle aziendali di posta elettronica per evitare la trasmissione di documenti e allegati vari al di fuori della attività connesse alla operatività aziendale.
un protocollo di utilizzo di Internet e dei social media in rete per evitare accessi al di fuori della attività connesse alla operatività aziendale.
un protocollo di limitazione della partecipazione, con la propria postazione aziendale, a blog, dibattiti e forum non attinenti alla operatività aziendale.
un protocollo di divieto di installare, sulle dotazioni HW rese disponibili, programmi SW e applicazioni scaricate dalla rete o caricate da fonti esterne, anche provvisti di regolare licenza, per le quali non sia stata concessa esplicita autorizzazione.
la verifica, nel rispetto delle norme che disciplinano tale materia, le condizioni di impiego e di mantenimento, da parte del personale, dei personal computer, notebook, palmari, telefoni cellulari dati in dotazione, penne ottiche
la verifica periodica dell'applicazione e dell'efficacia dei protocolli e delle procedure adottate.
l'esame di eventuali segnalazioni specifiche di nuove forme di reato o violazione dei sistemi informatici da qualsiasi fonte provenienti e il conseguente accertamento ritenuto necessario in conseguenza delle segnalazioni ricevute)
la tempestiva comunicazione all'OdV delle eventuali falle o violazioni dei sistemi.

la comunicazione all'OdV delle operazioni eventualmente effettuate in deroga ai principi sopra elencati.
Altro

B. AREA DEL NON FARE
9.2. - Relativamente ai reati informatici (art. 24 bis) è fatto divieto per tutti, posizioni apicali, dipendenti e collaboratori di:
porre in essere comportamenti in violazione delle prescrizioni di legge e aziendali relativamente all'uso di attrezzature informatiche, reti, server, HW e SW installati nei luoghi di lavoro
porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reati informatici, possano essere potenzialmente rischiose o comunque dannosi per la società
accedere a risorse informatiche a cui non si è autorizzati
alterare in qualsiasi modo, manomettere o modificare autonomamente i sistemi applicativi, le infrastrutture hardware e i dati in uso, di proprietà o di terzi, o manipolarne i dati
effettuare interventi manutentivi e di pulizia delle dotazioni, di iniziativa personale, senza informare il personale preposto agli interventi specifici ai quali è fatto obbligo segnalare eventuali malfunzionamenti
effettuare collegamenti alla rete con modalità difformi dall'architettura informatica prevista, mettendo a rischio la sicurezza dell'intero sistema informatico aziendale
predisporre, rappresentare o comunicare documenti informatici falsi o comunque suscettibili di fornire dati e informazioni non rispondenti alla realtà o in danno alla azienda
utilizzare password private non autorizzate e controllate dal personale preposto agli interventi specifici
cedere a terzi o non conservare correttamente le proprie credenziali di autenticazione
danneggiare i sistemi informatici di proprietà o di terzi
installare programmi non autorizzati e/o privi di regolare licenza, inducendo il rischio di diffondere virus informatici o sanzioni a carico della società per le eventuali violazioni alle norme a tutela del diritto d'autore
scaricare programmi dalla rete, anche tramite download gratuito, senza specifica autorizzazione della società e previa ricognizione tecnica delle articolazioni aziendali preposte agli specifici servizi
utilizzare la propria casella di posta elettronica per chat, trasmissioni di documenti e allegati vari al di fuori della attività connesse alla operatività aziendale
prendere parte a blog, dibattiti e forum non attinenti al lavoro con la propria postazione aziendale di accesso alla rete.
lasciare la propria postazione di lavoro senza aver preso tutte le cautele necessarie a conservare la segretezza del loro identificativo e della loro password e impedire che informazioni riservate possano essere visualizzate da soggetti non autorizzati

precostituire documenti/dati falsi o alterati per consentire/ effettuare operazioni informatiche al di fuori delle modalità aziendali approvate e di legge
accedere in maniera non autorizzata ai sistemi informativi interni per operare alterare informazioni e/o disposizioni al di fuori delle modalità standard approvate e di legge
avere un comportamento non collaborativo con le Autorità competenti in sede ispettiva o con le Autorità Giudiziarie
i divieti sopra rappresentati si intendono estesi anche ad attività informatiche effettuate in via indiretta attraverso operazioni concertate con terzi
altro

10. PRINCIPI E STANDARD DI CONTROLLO IN RELAZIONE AI REATI CONTRO LA PERSONALITÀ INDIVIDUALE

I reati contro la personalità individuale possono apparire, in linea di massima, non attinenti a fattispecie pertinenti al contesto Isfort.

L'articolo 25-quinquies del decreto 231 contempla, infatti, principalmente reati sessuali, di sfruttamento della prostituzione, pedopornografia, detenzione di materiale pornografico, ma anche intermediazione illecita e sfruttamento del lavoro.

E' evidente che l'intermediazione illecita, la creazione di opportunità di lavoro non rispondenti alle norme ovvero lo sfruttamento, in termini di remunerazione o di mancato rispetto delle norme giuslavoristiche e dei CCNL applicati sono le tipologie più comuni a una azienda ma non va affatto sottovalutato il rischio che persone in posizione apicale o subordinata possano commettere reati di pornografia minorile e di detenzione e scambio di materiale pornografico agevolati dalla possibilità di accedere a social media e a Internet attraverso i sistemi informatici aziendali.

A. AREA DEL FARE
10.1. – Su queste basi in Isfort il sistema di controllo dei reati contro la personalità individuale (art. 25 – quinquies) prevede:
un protocollo delle principali fasi del processo di selezione ed assunzione di personale, individuando i soggetti coinvolti nella gestione di tale attività, nonché le attività relative al riconoscimento di bonus o incentivi a dipendenti.
il rispetto delle norme giuslavoriste e degli accordi sindacali per l'assunzione e il rapporto di lavoro in generale
il divieto di convenire retribuzioni inferiori a quelle fissate dai contratti collettivi sulla base delle responsabilità e dei compiti della mansione attribuita al dipendente e comunque in riferimento ai valori medi di mercato.
l'assunzione di nuove risorse umane e/o gli avanzamenti di carriera sulla base di valutazioni oggettive in merito alle competenze possedute e a quelle potenzialmente esprimibili in relazione alla funzione da ricoprire.
un'apposita dichiarazione, da parte del personale tutto e nei contratti con i collaboratori esterni, in cui si affermi, da parte dei medesimi, di essere a conoscenza e di accettare, nella sua generalità, il Codice etico dell'azienda.
il rispetto delle regole di correttezza e di buon comportamento nell'ambiente di lavoro con particolare attenzione a situazioni lavorative anormali o abnormi.
il rifiuto di qualunque atteggiamento che discrimini personale e collaboratori per ragioni politiche e sindacali, di fede religiosa, razziali, di lingua, di sesso, di età o handicap.
il divieto di accogliere raccomandazioni e pressioni per favorire assunzioni e/o avanzamenti di carriera oltre le valutazioni oggettive di merito.
il divieto di approfittare della propria posizione aziendale per indurre comportamenti lesivi della dignità personale o conseguire indebiti vantaggi a titolo personale.

il divieto di affidarsi a intermediari di lavoro non autorizzati e riconosciuti o a forme di intermediazione illecita.
il divieto remunerare prestazioni lavorative con favori e beni materiali, anche sotto forma monetaria non contrattualizzata.
il divieto di diffondere dati personali, documenti riservati o confidenziali, legati alla persona con riferimento alle norme sulla privacy.
la diffusione, la conoscenza e il rispetto da parte dei dipendenti, dei contenuti del Modello e del Codice Etico in relazione ai reati intermediazione illecita e sfruttamento del lavoro.
la diffusione, la conoscenza e il rispetto da parte dei dipendenti dei contenuti del Modello e del Codice etico, con particolare riferimento alle fattispecie di reati sessuali, di sfruttamento della prostituzione, pedopornografia, detenzione di materiale pornografico.
il divieto di utilizzo della posta elettronica, Internet, social media, blog e forum, attraverso i sistemi informatici aziendali, per trasmettere, ricevere e scambiare materiale pornografico.
il divieto di installare, sulle dotazioni HW rese disponibili, programmi SW e applicazioni scaricate dalla rete o caricate da fonti esterne, avente oggetto materiale pornografico.
Il divieto di utilizzare i personal computer, notebook, palmari, telefoni cellulari dati in dotazione, penne ottiche per la trasmissione o scambio di materiale pornografico.
la verifica periodica dell'applicazione e dell'efficacia dei protocolli e delle procedure adottate.
l'esame di eventuali segnalazioni specifiche di nuove forme di reato in materi di reati contro la personalità individuale da qualsiasi fonte provenienti e il conseguente accertamento ritenuto necessario in conseguenza delle segnalazioni ricevute.
la tempestiva comunicazione all'OdV delle eventuali falle o violazioni del processo di controllo dei reati contro la personalità individuale.
la comunicazione all'OdV delle operazioni eventualmente effettuate in deroga ai principi sopra elencati.
Altro

B. AREA DEL NON FARE
10.2. - Relativamente ai reati contro la personalità individuale (art. 25 – quinquies) è fatto divieto per tutti, posizioni apicali, dipendenti e collaboratori di:
porre in essere comportamenti in violazione delle prescrizioni di legge e aziendali relativamente ai reati contro la personalità individuale
porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reati contro la personalità individuale, possano essere potenzialmente lesivi della dignità della persona e, comunque dannosi per la società, con specifico riferimento a motivazioni di genere, politiche e sindacali, di fede religiosa, razziali, di lingua, di sesso, di età o handicap
attuare disposizioni e comportamenti, in violazione della dignità della persona o comunque dannosi per la società, sulla base di ordini emanati da soggetto non competente e non legittimato ovvero sulla base di ordini inappropriati o illegali da parte di soggetto

legittimato. In tali casi, il dipendente e/o collaboratore deve dare immediata comunicazione dell'ordine o dell'atto direttivo ricevuto al proprio responsabile o referente ovvero all'organo amministrativo
accettare favori e beni materiali, sotto forma sia di prestazioni monetarie sia di regali di valore significativo in sostituzione delle forme di retribuzione lavorativa di legge e contrattuali.
accettare eventuali regali di cui sia manifesta e inequivocabile la natura strumentale o che eccedano, con il loro valore, le aspettative di un normale rapporto di cortesia e gratitudine
omettere, in caso di tentativi di subornazione da parte di posizioni apicali e superiori diretti, la denuncia ai referenti opportuni, per consentire, se del caso anche l'attivazione tempestiva dell'Organismo di vigilanza, al fine di stroncare sul nascere comportamenti illeciti e comunque difformi dallo spirito del Codice Etico
utilizzare la posta elettronica, Internet, social media, blog e forum, attraverso i sistemi informatici aziendali, per trasmettere, ricevere e scambiare materiale pornografico
installare, sulle dotazioni HW rese disponibili, programmi SW e applicazioni scaricate dalla rete o caricate da fonti esterne, avente oggetto materiale pornografico
utilizzare i personal computer, notebook, palmari, telefoni cellulari dati in dotazione, penne ottiche per la trasmissione o scambio di materiale pornografico
accedere in maniera non autorizzata ai sistemi informativi interni per operare alterare informazioni e/o disposizioni in relazione ai reati contro la personalità individuale
avere un comportamento non collaborativo con le Autorità competenti in sede ispettiva o con le Autorità Giudiziarie
i divieti sopra rappresentati si intendono estesi anche ad attività informatiche e non effettuate in via indiretta attraverso operazioni concertate con terzi
altro

11. PRINCIPI E STANDARD DI CONTROLLO IN RELAZIONE AI REATI TRIBUTARI

La legge 19 dicembre 2019, n.157 e il successivo D.Lgs. 15 luglio 2020, n. 75, hanno inserito gli illeciti tributari nel D.Lgs. n. 231/2001 (art. 25 quinquesdecies), innalzando contestualmente le pene minime e massime, abbassando le soglie di rilevanza penale dell'imposta evasa o dell'imponibile sottratto all'imposizione, per specifici delitti tributari.

La normativa è in ulteriore evoluzione come attestato dalla previsione di misure di rafforzamento del regime di *adempimento collaborativo in materia fiscale* tra le proposte contenute nel c.d. Piano Colao, redatto dal comitato di esperti in materia economica e sociale, voluto dal governo per elaborare proposte volte al rilancio del paese a seguito dell'emergenza Covid, consegnato, a luglio 2020, alla presidenza del Consiglio.

I reati presupposto 231 in materia tributaria sono pertanto diventati:

- dichiarazione fraudolenta mediante fatture per operazioni inesistenti;
- dichiarazione fraudolenta mediante altri artifici;
- emissione di fatture o altri documenti per operazioni inesistenti;
- occultamento o distruzione di documenti contabili;
- sottrazione fraudolenta al pagamento delle imposte.
- dichiarazione infedele
- omessa dichiarazione
- indebita compensazione
- ipotesi di delitto tentato e non consumato

Questi aggiornamenti rientrano nell'ambito dell'accresciuta attenzione rivolta dalle istituzioni europee alla modalità di gestione fiscale dell'impresa (Direttiva PIF, UE n. 2017/1371), Protezione degli interessi finanziari), all'analisi dei sistemi di controllo e alla conseguente mappatura di processi a rischio.

La tematica introduce, inoltre, la possibilità che l'azienda in parallelo alla redazione del MOG 231 possa ritenere di rafforzare il proprio presidio del rischio fiscale attraverso un modello di controllo strutturato, comunemente definito *Tax Control Framework (TCF)*, che prevede *un regime di adempimento collaborativo* con l'Agenzia delle Entrate.

A prescindere dalla effettiva adozione della proposta Colao di incentivo all'adozione del TCF, appare palese come la gestione del rischio fiscale per le imprese, già obbligata alla luce delle modifiche apportate, sul finire del 2019, al D.lgs. 231/2001, è ormai elemento portante del sistema di *compliance* aziendale.

B. AREA DEL FARE
11.1. – Su queste basi in Isfort il sistema di controllo in relazione ai reati tributari (art. 25 quinquiesdecies) prevede:

la definizione dell'assetto organizzativo della società, con riferimento alle responsabilità fiscali.
l'analisi approfondita di tutti i processi aziendali allo scopo di individuare le aree interessate dai possibili rischi fiscali.
la vigilanza sulle attività sensibili tipicamente svolte nell'ambito del processo fiscale, direttamente rilevanti ai fini della commissione dei reati tributari (es. la predisposizione delle dichiarazioni fiscali IRES e IVA).
la vigilanza sulle attività sensibili svolte al di fuori del processo fiscale, ma nell'ambito delle quali è possibile commettere direttamente uno o più dei reati tributari 231 (es. gestione della contabilità, tenuta e custodia della documentazione obbligatoria e delle scritture contabili, etc.).
la vigilanza sulle attività sensibili svolte nell'ambito di processi operativi ma con riflessi sul processo fiscale e potenzialmente rilevanti per la commissione dei reati tributari. (es. gestione acquisti di beni e servizi, gestione vendite di beni e servizi", gestione del magazzino)
la mappatura dei relativi controlli, incluse le attività di testing periodiche (es. semestrali o annuali) sui controlli identificati e forme di reporting periodico alle figure apicali preposte.
l'introduzione di una figura dedicata a curare l'attuazione e l'aggiornamento del modello di controllo dei rischi fiscali e il monitoraggio dei rischi individuati (cd. Tax Risk Manager).
l'attuazione di un piano di comunicazione, informazione e formazione per promuoverne la consapevolezza tra i dipendenti e le parti interessate in merito ai comportamenti illeciti, elusivi ed evasivi in ambito amministrativo e fiscale.
la diffusione, la conoscenza e il rispetto da parte dei dipendenti, dei contenuti del Modello e del Codice Etico in relazione ai reati tributari.
l'esame di eventuali segnalazioni specifiche di nuove forme di reato in materi di reati tributari da qualsiasi fonte provenienti e il conseguente accertamento ritenuto necessario in conseguenza delle segnalazioni ricevute.
la tempestiva comunicazione all'OdV delle eventuali falle o violazioni del processo di controllo dei reati tributari.
la comunicazione all'OdV delle operazioni eventualmente effettuate in deroga ai principi sopra elencati.
Altro

B. AREA DEL NON FARE
11.2. - Relativamente ai reati tributari (art. 25 quinquiesdecies) è fatto divieto per tutti, posizioni apicali, dipendenti e collaboratori di:
porre in essere comportamenti in violazione delle prescrizioni di legge e aziendali relativamente ai reati tributari
porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reati tributari, possano essere potenzialmente prefigurare la commissione di comportamenti evasivi o elusivi

attuare disposizioni e comportamenti comunque dannosi in materia tributaria per la società, sulla base di ordini emanati da soggetto non competente e non legittimato ovvero sulla base di ordini inappropriati o illegali da parte di soggetto legittimato. In tali casi, il dipendente e/o collaboratore deve dare immediata comunicazione dell'ordine o dell'atto direttivo ricevuto al proprio responsabile o referente ovvero all'organo amministrativo
omettere, in caso di tentativi di subornazione da parte di posizioni apicali e superiori diretti, la denuncia ai referenti opportuni, per consentire, se del caso anche l'attivazione tempestiva dell'Organismo di vigilanza, al fine di stroncare sul nascere comportamenti illeciti e comunque difformi dallo spirito del Codice Etico
accedere in maniera non autorizzata ai sistemi informativi interni per operare alterare informazioni e/o disposizioni in relazione ai reati tributari
avere un comportamento non collaborativo con le Autorità competenti in sede ispettiva o con le Autorità Giudiziarie
i divieti sopra rappresentati si intendono estesi anche ad attività e comportamenti effettuati in via indiretta attraverso operazioni concertate con terzi
altro

12. PRINCIPI E STANDARD DI CONTROLLO IN RELAZIONE A:
    a. reati ambientali (art.25 –undecies)
    b. reati in relazione all'impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 25-duodecies)
    c. razzismo e xenofobia (art. 25-terdecies)
    d. frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati (art. 25-quaterdecies)
    e. contrabbando (art. 25- sexiesdecies)

In linea di principio le fattispecie di reato descritte nel presente paragrafo **sembrano essere al di fuori delle aree di intervento della Isfort** che, peraltro il personale difficilmente può compiere in ambiti aziendali.

Unica eccezione appaiono **i reati ambientali**, che in Isfort, per la sua specificità non possono essere di fattispecie criminose rilevanti. Le attività di servizi e l'ubicazione delle sedi i cui si svolgono dette attività, infatti, permettono di escludere la commissione di reati in materia di scarichi di acque reflue, di inquinamento del suolo o delle acque, di traffico illecito di rifiuti, di inquinamento atmosferico.

Le attività aziendali in materia ambientale sembrano essere limitate, dunque, alla **raccolta differenziata e allo smaltimento dei rifiuti solidi urbani, che al limite comportano sanzioni amministrative**.
Per queste motivazioni non si rende necessaria, al di là delle generali prescrizioni al personale sulla base delle **norme locali**, l'individuazione di una funzione aziendale di controllo delle operazioni di gestione e prevenzione dei rischi ambientali.

Unica menzione merita **il traffico di animali** che il legislatore ha voluto ricomprendere nei reati ambientali. Anche in questo caso si esclude che l'azienda possa incorrere in tale fattispecie di reato penale ed eventuali reati compiuti da un dipendente, con l'utilizzo di strutture aziendali, rientra esclusivamente nella responsabilità personale.

L'impiego di cittadini di paesi terzi il cui soggiorno è irregolare impegna la responsabilità della società, ai sensi del D.Lgs. 231/2001, solo ove sia commesso in forma dolosa e nella forma aggravata e appare, comunque, una fattispecie di reato del tutto al di fuori delle attività e dei processi aziendali altrettanto quanto la commissione di reati di razzismo e xenofobia, frode in competizioni sportive e esercizio di gioco abusivo e contrabbando.

13. CONCLUSIONI

A titolo meramente esemplificativo, e non di validazione di efficacia, di concerto con l'Organismo di Vigilanza, Isfort ha effettuata una valutazione del rischio di non compliance dei diversi sistemi di controllo adottati nel Modello di Organizzazione, Gestione e Controllo di Isfort senza che con ciò si sia inteso determinare una minore attenzione al dettato del D.Lgs 231/2001 e definire situazioni di minore attenzione ai fini del rischio di commissione di reati presupposto 231.

La valutazione del rischio di non compliance del modello 231, ovvero della situazione dei controlli aziendali, **attesi gli interventi integrativi e/o correttivi da parte dell'Organismo di Vigilanza**, conduce considerazioni esclusivamente **probabilistiche**, in assenza di indici e criteri generalmente accettati, e non può precostituire il giudizio complessivo sulla realtà portata del MOG aziendale, che può variare in ragione delle peculiarità operative dell'Istituto, dell'applicabilità di alcuni standard alla dimensione aziendale (numero dei dipendenti, quantità e peso delle operazioni, diffusione territoriale).

Coerentemente con quanto in precedenza Isfort **ha adottato, con delibera del Consiglio di Amministrazione del …….. 2021, anche in forma di protocollo**, quale preciso riferimento, idonea informativa e contestuale condivisione e sottoscrizione, da parte di tutti i destinatari, delle regole di condotta e dei comportamenti conseguenti, specifici e ineludibili, ai fini del rispetto del Decreto Legislativo 231/2001 e delle previsioni del Capitolo 5 – Sistema Disciplinare Interno e del Capitolo 6 - Piano di Formazione e Comunicazione del MOG e del Codice Etico della Parte generale del Modello, dandone idonea pubblicità in ambito aziendale e sul proprio sito internet www.isfort.it.

Di seguito si riepiloga il corpo dei principi e degli standard di controllo adottati dalla Società sui quali sarà esercitata **azione di aggiornamento periodico**, in particolare in occasione di:

- interventi normativi a modifica delle disposizioni contenute nel D. Lgs. 231/01, che possa aver impatto sulla definizione delle aree di rischio;
- modifica dei processi aziendali, da parte degli Organi sociali in concorso con l'Organismo di Vigilanza, a cui spettano, per legge (cfr. il capitolo 7 della Parte Generale), i compiti di vigilanza sul funzionamento, l'efficacia e l'osservanza del Modello, che implica la verifica della coerenza tra norme adottate e comportamenti concretamente attuati oltre che della adeguatezza dei medesimi rispetto alla realtà operativa aziendale.

PRINCIPI E STANDARD DI CONTROLLO ISFORT
4.1. - modalità di contatto del personale nei rapporti con la Pubblica Amministrazione
4.2. - comportamenti a rischio da evitare nei rapporti con i rappresentanti della PA

4.3. – comportamenti vietati nei confronti della PA
4.4. – congruità e volumi delle operazioni con la PA
5.1.1. – sistema di controllo dei flussi monetari e finanziari
5.1.2. – divieti relativi ai mezzi di pagamento delle operazioni di
5.2.1. - sistema di controllo della selezione e assunzione del personale
5.2.2. - divieti relativi alla selezione e assunzione del personale
5.3.1. – sistema di controllo del processo di gestione degli omaggi
5.3.2. - divieti relativi alla gestione degli omaggi
5.4.1. – sistema di controllo delle spese di rappresentanza
5.4.2. - divieti relativi alla gestione delle spese di rappresentanza
5.5.1. – sistema di controllo degli incarichi di consulenza e prestazioni professionali
5.5.2. - divieti relativi al conferimento di incarichi di consulenza e prestazioni professionali
5.6.1. – sistema di controllo degli acquisti di beni e servizi
5.6.2. - divieti relativi agli acquisti di beni e servizi
5.7.1. – sistema di controllo delle sponsorizzazioni prevede
5.7.2. - divieti relativi alle sponsorizzazioni
6. 1. – sistema di controllo dei reati societari
6.2. – divieti relativi ai reati societari
7.1. – sistema di controllo dei reati di riciclaggio e ricettazione
7.2. - divieti relativi ai reati di riciclaggio e ricettazione
8.1. – sistema di controllo dei reati in materia di sicurezza sul lavoro
8.2. - divieti relativi ai reati dei reati in materia di sicurezza sul lavoro
9.1. – sistema di controllo dei reati informatici
9.2. - divieti relativi ai reati informatici
10.1. – sistema di controllo dei reati contro la personalità individuale
10.2. – divieti relativi ai reati contro la personalità individuale
11.1. – sistema di controllo dei reati tributari
11.2. – divieti relativi ai reati tributari

12. standard di controllo in relazione a reati ambientali, reati in relazione all'impiego di cittadini di paesi terzi il cui soggiorno è irregolare, razzismo e xenofobia, frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati, contrabbando