INNOVHUB
STAZIONI SPERIMENTALI
PER L'INDUSTRIA

Innovazione e ricerca

SSCCP
STAZIONE SPERIMENTALE
CARTA, CARTONI E PASTE PER CARTA

SSC
STAZIONE SPERIMENTALE
PER I COMBUSTIBILI

SSOG
STAZIONE SPERIMENTALE
PER LE INDUSTRIE DEGLI OLI E DEI GRASSI

SSS
STAZIONE SPERIMENTALE
PER LA SETA

Modello di Organizzazione, gestione e controllo per la prevenzione dei reati

(d. lgs. n. 231/2001)

Approvato con Determina del Presidente n. 9 del 31/1/2018

PARTE SPECIALE

PREMESSA

La Parte Speciale del Modello ha la finalità di definire linee, regole e principi di comportamento che tutti i destinatari del Modello dovranno seguire al fine di prevenire, nell'ambito delle specifiche attività sensibili svolte nell'Azienda, la commissione dei reati previsti dal Decreto, e di assicurare condizioni di correttezza e trasparenza nella conduzione delle attività aziendali.

Nello specifico, la Parte Speciale del Modello ha lo scopo di:
- Individuare, sulla base della descrizione delle fattispecie incriminatrici, le attività dell'Azienda nell'ambito delle quali è presente un rischio di commissione dei reati rilevanti ai sensi del Decreto (attività sensibili);
- indicare le modalità che gli esponenti aziendali sono chiamati a osservare ai fini della corretta applicazione del Modello;
- disciplinare i comportamenti richiesti dai destinatari del Modello al fine di prevenire la commissione dei reati;
- fornire all'Organismo di Vigilanza e alle altre funzioni di controllo gli strumenti per esercitare le attività di monitoraggio, controllo e verifica.

Pertanto, nella Parte Speciale, che segue, saranno analizzate le attività considerate come "sensibili" ai fini del Decreto in relazione al tipo di attività svolta da Innovhub SSI, di seguito anche Azienda.
Saranno in particolare analizzate le attività che presentano profili di rischiosità in relazione a quanto emerso dalla Gap Analysis.
Sono individuate, conseguentemente, linee guida di comportamento che traducono operativamente quanto espresso, in termini di principi, nel Codice Etico.
In particolare, sono identificati, "comportamenti corretti" e "comportamenti errati".
Inoltre, gli aspetti operativi, per la gestione delle attività volte alla prevenzione dei reati, sono dettagliati in procedure operative integrate nel sistema qualità dell'Azienda.
A seguito dell'adozione del Piano di Prevenzione della Corruzione (in allegato) da parte di Innovhub SSI, i protocolli e le procedure di seguito elencati, adottati dall'Azienda a presidio dei rischi relativi ai reati elencati nel d. lgs. 231/2001, varranno anche, ove pertinenti, per i reati elencati nella legge 190/2012 in tema di prevenzione della corruzione.
Si rimanda, per quanto attiene alla descrizione delle singole fattispecie di reato, all'Allegato 1 contenente l'elenco dei reati con le norme incriminatrici.

PRINCIPI DI CONTROLLO

Per tutte le tipologie di reato
Per impedire la commissione dei reati è necessario organizzare un sistema che rispetti una serie di protocolli di controllo generale, quali a titolo esemplificativo:
- Segregazione dei compiti: il sistema garantisce l'applicazione del principio di separazione delle funzioni.

In base a ciò:

- A nessuno vengono attribuiti poteri illimitati;
- I poteri e le responsabilità sono chiaramente definiti e conosciuti all'interno dell'organizzazione;
- I poteri autorizzativi e di firma sono coerenti con le responsabilità organizzative assegnate. Tale segregazione è garantita dall'intervento, all'interno dello stesso macro processo aziendale, di più soggetti al fine di garantire indipendenza e obiettività dei processi. La separazione delle funzioni è attuata, sia pure in modo parziale, anche attraverso l'utilizzo di sistemi informatici che abilitano certe operazioni solo a persone identificate e autorizzate. La segregazione è valutata considerando l'attività sensibile nel contesto dello specifico processo di appartenenza e tenuto conto della complessità della medesima attività.

- Tracciabilità: per ogni operazione è disponibile un adeguato supporto documentale su cui si può procedere in ogni momento a controlli che identifichino le caratteristiche e le motivazioni dell'operazione, chi ha autorizzato, effettuato, registrato, verificato le operazioni eseguite; sono disciplinati in modo dettagliato i casi in cui si può procedere alla cancellazione o distruzione delle registrazioni effettuate. La salvaguardia di dati e procedure in ambito informatico è assicurata mediante l'adozione delle misure di sicurezza già previste dal d. lgs 196/2003 (Codice in materia di protezione dei dati personali) per tutti i trattamenti di dati effettuati con strumenti elettronici;

- Procure e deleghe: i poteri autorizzativi e di firma assegnati sono:
  - coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, indicazione delle soglie di approvazione delle spese;
  - chiaramente definiti e conosciuti all'interno dell'Azienda. Sono definiti i ruoli aziendali ai quali è assegnato il potere di impegnare l'Azienda in determinate spese specificando i limiti e la natura delle spese. L'atto attributivo di funzioni deve rispettare gli specifici requisiti eventualmente richiesti dalla legge.

- Attività di monitoraggio: è finalizzata all'aggiornamento periodico di procure, deleghe di funzione, nonché del sistema di controllo, in coerenza con il sistema decisionale e con l'intero impianto della struttura organizzativa;

- Regolamentazione: è prevista l'esistenza di disposizioni idonee a fornire principi di comportamento, modalità operative per lo svolgimento di attività sensibili nonché modalità di archiviazione della documentazione rilevante.

COMPITI DELL'ORGANISMO DI VIGILANZA

Compiti specifici dell'O.d.V. concernenti l'osservanza e l'efficacia del Modello in materia di reati societari sensibili ai sensi del d. lgs. 231/01:

- monitorare l'efficacia e l'effettiva attuazione di quanto previsto in ordine alla prevenzione dei reati sensibili, anche attraverso verifiche periodiche;

- curare l'attività di formazione periodica sui nelle attività sensibili della presente Parte Speciale;
- esaminare le eventuali segnalazioni provenienti dagli organi di controllo (Collegio dei Revisori) o da qualsiasi dipendente e disporre gli accertamenti ritenuti necessari od opportuni;
- conservare la documentazione relativa ai controlli posti in essere nelle aree di rischio di cui alla presente Parte Speciale.

Nell'espletamento dei suddetti compiti, l'Organismo di Vigilanza ha libero accesso a tutta la documentazione relativa ai processi sensibili della Parte Speciale.

Nel caso in cui, dagli accertamenti svolti dall'Organismo di Vigilanza, emergano elementi che facciano risalire la violazione dei principi e protocolli contenuti nella presente Parte Speciale del Modello, la commissione del reato, o il tentativo di commissione del reato, direttamente al Rappresentante legale o a un membro del Consiglio di Amministrazione, l'Organismo di Vigilanza dovrà riferire all'intero Consiglio di Amministrazione per l'adozione degli opportuni adempimenti del caso.

PARTE SPECIALE "A"

Reati nei confronti della Pubblica Amministrazione (articoli 24 e 25 del Decreto)

A. 1 TIPOLOGIA DEI REATI

I reati attualmente previsti dal Decreto nei confronti della Pubblica Amministrazione sono:

- **Malversazione a danno dello Stato (art. 316-bis c.p.)**
- **Indebita percezione di erogazioni a danno dello Stato (art. 316-ter c.p.)**
- **Concussione (art. 317 c.p.)**
- **Corruzione per l'esercizio della funzione (art. 318 c.p.)**
- **Corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.)**
- **Corruzione in atti giudiziari (art. 319-ter c.p.)**
- **Induzione indebita a dare o promettere utilità (art. 319- quater c.p)**
- **Corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.)**
- **Istigazione alla corruzione (art. 322 c.p.)**
- **Peculato, concussione, induzione indebita dare o promettere utilità, corruzione e istigazione alla corruzione di membri degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri (art. 322-bis c.p.)**
- **Truffa (in danno dello Stato o di un altro ente pubblico) (art. 640 comma 2 n. 1 c.p.)**
- **Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.)**
- **Frode informatica in danno dello Stato o di altro Ente Pubblico (art. 640-ter c.p.)**
- **Corruzione tra privati (art, 2635 c.c.)**

A. 2 AREE DI RISCHIO

In considerazione dei rapporti che Innovhub SSI intrattiene, in ragione della propria attività, con soggetti e autorità pubbliche o incaricati di un pubblico servizio, le attività ritenute più specificamente a rischio alla luce della valutazione dei rischi effettuata, sono a titolo esemplificativo e non esaustivo le seguenti:

- negoziazione, stipulazione ed esecuzione di contratti e/o convenzioni con soggetti pubblici mediante partecipazione a bandi o con soggetti privati;
- gestione dei rapporti con soggetti pubblici per l'ottenimento di autorizzazioni e licenze necessari per lo svolgimento dell'attività;

- richiesta, acquisizione e gestione di contributi, sovvenzioni, finanziamenti erogati da soggetti pubblici;
- gestione di ispezioni e verifiche da parte di soggetti pubblici (es. ASL; Vigili del Fuoco; Guardia di Finanza; Ispettorato del Lavoro; Regione Lombardia e altri enti finanziatori);
- eventuale gestione/prestazione di servizi per soggetti terzi.

I reati maggiormente riferibili a quest' area sono quelli di corruzione (per un atto d'ufficio o per un atto contrario ai doveri d'ufficio) e di istigazione alla corruzione, che si realizzano attraverso l'offerta o la promessa di denaro o altra utilità agli interlocutori dell'ente che indice il bando per ottenere, indebitamente, l'aggiudicazione dello stesso o l'accelerazione indebita di un atto dovuto.

La condotta illecita si può realizzare anche attraverso la presentazione di documenti o dati volutamente falsi e/o lacunosi per ottenere l'aggiudicazione del finanziamento (truffa in danno di un ente pubblico).

Inoltre, sono da considerare i reati di corruzione tra privati nel caso di fornitura di una prestazione o di acquisto di un bene o un servizio a condizioni alterate rispetto a quelle di mercato.

Queste condotte possono generare sanzioni a carico di Innovhub SSI anche se poste in essere sotto forma di tentativo, salvo che l'Azienda non impedisca volontariamente il compimento dell'azione o la realizzazione dell'evento.

A. 3 PRINCIPI GENERALI DI COMPORTAMENTO

Alla luce di quanto sopra, sono di seguito espressamente indicati i comportamenti da tenersi da parte dei Destinatari del Modello, in via generale, nei rapporti con la Pubblica Amministrazione:

- osservare rigorosamente tutte le leggi e i regolamenti che disciplinano l'attività di Innovhub SSI, con particolare riferimento alle attività che comportano contatti e rapporti di qualsiasi natura con la Pubblica Amministrazione e con soggetti privati;
- instaurare e mantenere qualsiasi rapporto con la Pubblica Amministrazione e con soggetti privati sulla base di criteri di massima correttezza e trasparenza, in considerazione dell'imparzialità che deve ispirare l'attività amministrativa.

Si prevede, conseguentemente, l'espresso divieto per i Destinatari in tutte le aree a rischio di:

- porre in essere comportamenti tali da integrare le fattispecie di reato previste dagli artt. 24 e 25 del Decreto;
- porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo.

In particolare, è fatto espresso divieto di:

- effettuare elargizioni in denaro a pubblici ufficiali o incaricati di pubblico servizio o a clienti e fornitori;
- distribuire omaggi e regali a clienti pubblici, a clienti o fornitori privati al di fuori di quanto previsto dalla prassi di Innovhub SSI;
- accordare altri vantaggi di qualsiasi natura (come, a puro titolo di esempio, promesse di assunzioni o consulenze dirette o di prossimi congiunti) in favore di rappresentanti della Pubblica Amministrazione, a clienti o fornitori privati finalizzate comunque a ottenere illeciti vantaggi;
- riconoscere compensi in favore di consulenti e collaboratori esterni, in particolare in rapporti con enti pubblici o privati, che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o che, addirittura, non corrispondano ad alcuna prestazione;
- ricevere o sollecitare elargizioni in denaro, omaggi, regali, o vantaggi di altra natura da pubblici funzionari o soggetti privati, ove eccedano le normali pratiche commerciali e di cortesia; chiunque riceva omaggi o vantaggi di altra natura non compresi nelle c.d. "regalie d'uso" è tenuto a darne immediata comunicazione all'Organismo di Vigilanza;
- assumere personale e/o attribuire incarichi (ad es. di consulenza) nei casi in cui l'assunzione o l'incarico siano (o possano apparire) finalizzati allo scambio di favori con soggetti pubblici o con soggetti privati con i quali siano in essere contratti di vendita di servizi o acquisto di prestazioni o beni;
- rendere dichiarazioni mendaci all'autorità giudiziaria - questo principio di comportamento è trasversale ed applicabile a tutti i reati contemplati nella parte speciale - (art. 377 bis c.p.).
- falsificare documenti informatici pubblici e privati- questo principio di comportamento è trasversale ed applicabile a tutti i reati contemplati nella parte speciale - (art. 491 bis c.p.).

I consulenti esterni incaricati da Innovhub SSI e coinvolti nelle aree a rischio della presente Parte Speciale A devono sottoscrivere, in sede di contratto, una dichiarazione nella quale affermino: i) di conoscere il contenuto del d. lgs 231/01, del Codice Etico e dei principi del Modello di Innovhub SSI e di impegnarsi a osservarne il contenuto; ii) di segnalare tempestivamente all'O.d.V. di Innovhub SSI eventuali violazioni delle prescrizioni contenute nel Modello e nel Codice Etico dell'Azienda o di comportamenti comunque contrari a quanto previsto dal d. lgs 231/01 dei quali siano venuti a conoscenza nell'ambito dei rapporti con la Pubblica Amministrazione.

A. 4 PROTOCOLLI SPECIFICI DI COMPORTAMENTO

A. 4.1 Negoziazione, stipulazione ed esecuzione di contratti e/o convenzioni con soggetti pubblici e privati

Premessa

Il presente protocollo è destinato ai soggetti coinvolti nella partecipazione di Innovhub SSI a bandi indetti da soggetti pubblici per la fornitura di beni o servizi, nonché contratti di erogazione di prestazioni o di acquisto di beni o di servizi con soggetti privati.

Il protocollo è volto a garantire il rispetto da parte dell'Azienda, oltre che della normativa vigente, dei principi di trasparenza, correttezza, oggettività e verificabilità dell'attività.

Processi sensibili e rischi di reato

I reati maggiormente riferibili a questo settore di attività sono quelli di corruzione e truffa in danno di ente pubblico e corruzione tra privati.

A. 4.2 Richiesta di autorizzazione e licenze per l'attività aziendale

Premessa

Il presente protocollo è destinato ai soggetti coinvolti nella richiesta di autorizzazioni e licenze necessarie per lo svolgimento dell'attività aziendale.

L'attività riguarda, a titolo esemplificativo e non esaustivo, gli adempimenti in materia di lavoro e previdenza, le comunicazioni con le Camere di Commercio, le richieste di licenze e autorizzazioni in materia di ambiente e sicurezza (autorizzazione integrata ambientale, C.P.I.), rapporti con Comuni per pratiche edilizie.

Processi sensibili e rischi di reato

L'attività nell'area in esame riguarda in particolare la predisposizione e l'invio della documentazione richiesta; l'archiviazione della pratica; la gestione dei rapporti con l'ente pubblico di riferimento; la gestione di eventuali verifiche e ispezioni (vedi par. 4.3).

Principi di controllo

A. 4.3 Gestione di ispezioni e verifiche da parte di soggetti pubblici

Premessa

Il presente protocollo si applica ai soggetti coinvolti nelle ispezioni e/o verifiche da parte di soggetti pubblici sull'attività di Innovhub SSI.

Processi sensibili e rischi di reato

I reati di corruzione e truffa in danno di un ente pubblico possono essere commessi anche

dell'ambito delle ispezioni o verifiche da parte degli enti preposti, attraverso l'offerta di denaro o altra utilità o la comunicazione di dati o documenti non veritieri in relazione all'area sottoposta a verifica.

Principi di controllo

A. 4.4 Acquisizione e gestione di contributi, sovvenzioni, finanziamenti erogati da soggetti pubblici

Premessa

Il presente protocollo si applica ai soggetti coinvolti nella richiesta di contributi o finanziamenti in favore dell'attività aziendale erogati da enti pubblici (quali a titolo esemplificativo e non esaustivo finanziamenti fondi regionali L. 236/93, FSE, Fondi Interprofessionali etc.).

Il protocollo è volto a garantire il rispetto da parte dell'Azienda, oltre che della normativa vigente, dei principi di trasparenza, correttezza, oggettività e verificabilità dell'attività.

Processi sensibili e rischi di reato

La predisposizione di dati non veritieri nella richiesta di finanziamento (modalità di richiesta del finanziamento) o la destinazione a fini differenti da quelli per i quali il finanziamento è stato ottenuto (modalità di gestione del finanziamento) possono integrare i reati di truffa in danno dell'ente pubblico, indebita percezione di erogazione o di malversazione nel caso in cui il finanziamento sia destinato a realizzare opere o attività di pubblico interesse.

PARTE SPECIALE "B" –
I Reati Societari
(art. 25-ter del Decreto)

B. 1 TIPOLOGIA DEI REATI

I reati societari attualmente previsti nel Decreto sono i seguenti:

- **False comunicazioni sociali (art. 2621 c.c.)**
- **False comunicazioni sociali in danno della Società, dei soci o dei creditori (art. 2622 c.c.)**
- **Falsità nelle relazioni o nelle comunicazioni delle Società di revisione (art. 2624 c.c.)**

- **Impedito controllo (art. 2625 c.c.)**
- **Indebita restituzione dei conferimenti (art. 2626 c.c.)**
- **Illegale ripartizione degli utili e degli 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.)**
- **Omessa comunicazione del conflitto d'interesse (art. 2629-bis c.c.)**
- **Formazione fittizia del capitale (art. 2632 c.c.)**
- **Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.)**
- **Illecita influenza sull'assemblea (art. 2636 c.c.)**
- **Aggiotaggio (art. 2637 c.c.)**
- **Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638 c.c.)**

B. 2 AREE DI RISCHIO

Le aree di attività ritenute maggiormente a rischio per l'Azienda in relazione ai reati societari sono considerate le seguenti:

a) tenuta della contabilità, redazione del bilancio e delle altre relazioni e comunicazioni sociali in genere;

b) gestione delle incombenze societarie di competenza delle Aziende Speciali;

c) gestione dei rapporti con il CdA e con il Collegio dei Revisori.

B. 3 PRINCIPI GENERALI DI COMPORTAMENTO

Si prevede l'espresso divieto a carico dei Destinatari del Modello di:

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

B. 4 PROTOCOLLI SPECIFICI DI COMPORTAMENTO

B. 4.1 Predisposizione del bilancio

Premessa

Il presente protocollo è destinato a tutti i soggetti coinvolti a vario titolo nella formazione del bilancio dell'Azienda.

Il protocollo è volto a garantire il rispetto da parte dell'Azienda, oltre che della normativa vigente, dei principi di trasparenza, correttezza, oggettività e verificabilità dell'attività.

Processi sensibili e rischi di reato

I reati di false comunicazioni in danno dell'Azienda o dei creditori si realizzano principalmente (a titolo esemplificativo ma non esaustivo) attraverso l'inserimento nel bilancio e nelle altre comunicazioni previste dalla legge di dati non rispondenti al vero, anche se oggetto di valutazioni, che inducono in errore sulla reale situazione economica, patrimoniale e finanziaria dell'Azienda.

B. 4.2 Gestione dei rapporti con il Collegio dei revisori

Premessa

Il presente protocollo si applica ai membri del Consiglio di Amministrazione e a tutti gli uffici coinvolti nei rapporti con il Collegio dei revisori (nel caso in cui è previsto il coinvolgimento) nell'ambito delle attività svolte per legge dai predetti organismi.

Innovhub SSI garantisce la massima collaborazione e trasparenza nei rapporti e nelle comunicazioni con il Collegio dei revisori, nel rispetto della normativa vigente.

Processi sensibili e rischi di reato

Il rischio è quello di incorrere nel reato di impedito controllo nel caso in cui venga ostacolata l'attività del Collegio dei revisori, o di falsità nelle relazioni o nelle comunicazioni del Collegio dei Revisori nel caso in cui gli amministratori o altri soggetti aziendali inducano o istighino la condotta illecita del Collegio dei Revisori.

PARTE SPECIALE "C" –
I Delitti Informatici
(art. 24-bis del Decreto)

C. 1 TIPOLOGIA DEI REATI

I reati informatici attualmente previsti nel Decreto sono:

- **Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.)**
- **Detenzione e diffusione abusiva di codici di accesso a sistemi informatici e telematici (art. 615-quater c.p.)**
- **Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.)**

- **Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.)**
- **Installazione d'apparecchiature per intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.)**
- **Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.)**
- **Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter c.p.)**
- **Danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.)**
- **Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.)**
- **Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-quinquies c.p.)**

C. 2 AREE DI RISCHIO

L'area di attività ritenuta maggiormente a rischio in relazione ai reati informatici è la gestione del sistema informatico e telematico utilizzato in azienda.

C. 3 PROTOCOLLI SPECIFICI DI COMPORTAMENTO

Premessa

L'utilizzo del sistema informatico è disciplinato dalle Procedure del Sistema Qualità.

Le suddette procedure disciplinano e regolamentano le modalità di utilizzo delle apparecchiature informatiche e delle varie connessioni.

Processi sensibili e rischi di reato

Il sistema di gestione informatico e telematico deve garantire, attraverso la definizione dei requisiti di sicurezza informatica, la gestione degli accessi alle risorse informatiche e telematiche, il monitoraggio della sicurezza informatica e telematica, la protezione fisica e logica del server, che l'attività e l'invio di dati a sistemi telematici pubblici (es. Agenzia delle Entrate, INPS), sia svolta in sicurezza senza il rischio di incorrere in danneggiamenti del sistema o di sistemi altrui.

PARTE SPECIALE "D" - MODELLO EX ART. 30 D.Lgs 81/08
Reati in Tema di Tutela della Salute e
della Sicurezza sul Luogo di Lavoro

(art. 25-septies del Decreto)

D 1. TIPOLOGIA DEI REATI

I reati in materia di sicurezza sui luoghi di lavoro sono stati introdotti dall' 25-septies: Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro.

"1. In relazione al delitto di cui all'articolo 589 del codice penale, commesso con violazione dell'articolo 55, comma 2, del decreto legislativo attuativo della delega di cui alla Legge 3 agosto 2007, n. 123, in materia di salute e sicurezza sul lavoro, si applica una sanzione pecuniaria in misura pari a 1.000 quote. Nel caso di condanna per il delitto di cui al precedente periodo si applicano le sanzioni interdittive di cui all'articolo 9, comma 2, per una durata non inferiore a tre mesi e non superiore ad un anno. 2. Salvo quanto previsto dal comma 1, in relazione al delitto di cui all'articolo 589 del codice penale, commesso con violazione delle norme sulla tutela della salute e sicurezza sul lavoro, si applica una sanzione pecuniaria in misura non inferiore a 250 quote e non superiore a 500 quote. Nel caso di condanna per il delitto di cui al precedente periodo si applicano le sanzioni interdittive di cui all'articolo 9, comma 2, per una durata non inferiore a tre mesi e non superiore ad un anno. 3. In relazione al delitto di cui all'articolo 590, terzo comma, del codice penale, commesso con violazione delle norme sulla tutela della salute e sicurezza sul lavoro, si applica una sanzione pecuniaria in misura non superiore a 250 quote. Nel caso di condanna per il delitto di cui al precedente periodo si applicano le sanzioni interdittive di cui all'articolo 9, comma 2, per una durata non superiore a sei mesi".

I reati previsti dall'art. 25-septies del Decreto in materia di tutela della salute e della sicurezza sui luoghi di lavoro sono pertanto:

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

D 2. AREE DI RISCHIO

In questa Parte Speciale si fa riferimento alla complessiva gestione dell'igiene e sicurezza sui luoghi di lavoro nelle sedi di Innovhub SSI.

D 3. ADEMPIMENTI IN MATERIA DI SICUREZZA

Premessa

Innovhub SSI ha da sempre posto particolare attenzione al tema della sicurezza sui luoghi di lavoro.

L'Azienda si è attivata per raggiungere un livello organizzativo costantemente allineato con quanto richiesto dalla normativa vigente.

Lo sforzo dell'Azienda è continuativamente volto a garantire il miglior adempimento di tutti gli obblighi relativi al rispetto degli standard strutturali e tecnici per l'igiene e la sicurezza dei luoghi di lavoro e di natura organizzativa (quali, a titolo esemplificativo, emergenze, primo soccorso, riunioni periodiche della sicurezza), nonché alle verifiche periodiche sull'applicazione e l'efficacia delle misure attuate, anche con riguardo ad eventuali terzi operanti all'interno dell'azienda.

Conseguentemente, l'Azienda adotta nell'esercizio dell'impresa le misure che, secondo la particolarità dell'attività svolta, l'esperienza e la tecnica sono necessarie a tutelare l'integrità fisica e la personalità morale dei lavoratori.

La sicurezza nell'ambiente di lavoro si consegue con il coinvolgimento e la partecipazione di tutti coloro che operano all'interno dell'Azienda (datore di lavoro, dirigenti, preposti, prestatori di lavoro e loro rappresentanti) i quali devono tenere, nella loro attività quotidiana, un comportamento conforme alla legge e alle procedure aziendali.

La ricerca di vantaggi per l'Azienda, qualora comportino o possano comportare la violazione, dolosa o colposa, alle norme in tema di tutela della sicurezza e salute del lavoro, non è mai giustificata.

In conformità alla normativa vigente in materia di salute e sicurezza del lavoro, l'Azienda adotta un'organizzazione basata sui seguenti principi e norme di comportamento:

- evitare i rischi;
- valutare i rischi che non possono essere evitati;
- combattere i rischi alla fonte;
- adeguare il lavoro all'uomo, in particolare per quanto concerne la concezione dei posti di lavoro e la scelta delle attrezzature di lavoro e dei metodi di lavoro, in particolare per attenuare il lavoro monotono e il lavoro ripetitivo e per ridurre gli effetti di questi lavori sulla salute;
- tener conto del grado di evoluzione della tecnica;
- sostituire ciò che è pericoloso con ciò che non è pericoloso o che è meno pericoloso;
- programmare la prevenzione, mirando a un complesso coerente che integri nella medesima la tecnica, l'organizzazione del lavoro, le condizioni di lavoro, le relazioni sociali e l'influenza dei fattori dell'ambiente di lavoro;
- dare la priorità alle misure di protezione collettiva rispetto alle misure di protezione individuale;
- impartire adeguate istruzioni ai lavoratori.

La valutazione dei rischi

Tutti i siti hanno redatto il proprio Documento di Valutazione dei Rischi in ottemperanza a quanto previsto dall'art. 28 comma 2 del d. lgs 9 aprile 2008 n. 81, a conclusione della valutazione dei rischi condotta ai sensi dell'art. 28 comma 1.

Il Documento di Valutazione dei Rischi ha coinvolto tutta l'azienda attraverso l'analisi delle diverse mansioni e l'individuazione dei rischi e delle conseguenti misure di prevenzione.

I documenti contengono la descrizione dell'attività aziendale; la nomina delle figure del RSPP, del RLS e del Medico competente; l'individuazione delle Squadre di Pronto Intervento e Primo Soccorso Aziendale, la definizione del Piano d'Emergenza interno; la modalità di gestione della sicurezza in azienda.

Il processo di valutazione dei rischi contiene i criteri e la metodologia adottati, il procedimento di valutazione, l'individuazione delle misure idonee a prevenire i rischi.

Attività in appalto

Le procedure del Sistema Qualità Innovhub SSI indicano le regole che l'Azienda deve applicare nei casi in cui affidi attività in appalto ad aziende o lavoratori automi esterni.

In applicazione di quanto previsto dall'art. 26 del d. lgs n. 81/2008, Innovhub SSI fornisce dettagliate informazioni sui rischi specifici esistenti nell'ambiente di lavoro in cui sono destinati ad operare e sulle misure di prevenzione e di emergenza adottate all'interno degli stabilimenti.

In particolare Innovhub SSI all'atto della formalizzazione dell'incarico, provvede alle seguenti attività:

- esegue la verifica del possesso dei requisiti d'idoneità da parte dell'impresa appaltatrice o dei lavoratori autonomi, mediante l'iscrizione alla camera di commercio, industria e artigianato o l'autocertificazione;
- fornisce agli stessi soggetti dettagliate informazioni sui rischi specifici esistenti nell'ambiente in cui sono destinati ad operare e sulle misure di prevenzione e di emergenza adottate in relazione alla propria attività;
- dove richiesto, esegue la valutazione del rischio, elaborando il DUVRI (Documento Unico di Valutazione dei Rischi derivanti dalle Interferenze), nel quale sono identificate le misure di prevenzione e protezione dai rischi sul lavoro incidenti sull'attività lavorativa oggetto dell'appalto.

L'Ufficio preposto invia la documentazione all'appaltatore e la richiede controfirmata per presa visione. Le dichiarazioni vengono archiviate e inoltrate al RSPP.

L'azienda coopera con gli appaltatori all'attuazione delle misure di prevenzione e protezione dai rischi sul lavoro incidenti sull'attività lavorativa oggetto dell'appalto e coordina gli interventi di protezione e prevenzione dai rischi cui sono esposti i lavoratori, informandosi reciprocamente anche al fine di eliminare rischi dovuti alle interferenze tra i lavori delle diverse imprese coinvolte nell'esecuzione dell'opera complessiva.

Organizzazione

La struttura interna relativa alla gestione del sistema della sicurezza è definita nei Documenti di Valutazione dei Rischi.

Innovhub SSI ha recepito la designazione camerale del RSPP e del Medico Compente, e ha designato la squadra di emergenza. È prevista la formale designazione dell'RLS.

Controlli e azioni correttive: il RSPP e l'ASPP inviano un report annuale all'O.d.V. relativo all'andamento del sistema della sicurezza segnalando eventuali azioni di miglioramento.

Sono previste riunioni periodiche, tra O.d.V., RSPP, ASPP aventi ad oggetto: i) la verifica degli adempimenti sulla sicurezza; ii) il mantenimento degli standard previsti dalla normativa vigente e dalle procedure interne; iii) la verifica sull'idoneità di tutte le misure adottate.

La documentazione relativa all'attività di cui sopra e ai relativi controlli deve essere trasmessa, con apposito verbale redatto, all'O.d.V. affinché possa conservarla nel proprio archivio quale registrazione dell'attività svolta in materia di sicurezza.

Riesame della direzione: in ogni caso, l'O.d.V. propone all'organo dirigente il riesame e la modifica delle predette misure quando siano scoperte e/o segnalate significative violazioni delle norme relative alla prevenzione degli infortuni e all'igiene sul lavoro o in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico.

Formazione e informazione dei lavoratori: il Datore di Lavoro, in accordo con i soggetti responsabili della sicurezza, cura gli adempimenti relativi alla formazione e informazione del personale in materia di sicurezza e igiene dei luoghi di lavoro.

La documentazione relativa alla formazione/informazione e quella e ai conseguenti controlli è conservata dall'RSPP e trasmessa annualmente all'O.d.V., accompagnata da una nota contenente eventuali anomalie e/o criticità riscontrate.

Tutti i "nuovi lavoratori", così come definiti dall'art. 2 comma 1 lett. a) del d. lgs n. 81/2008, seguono appositi corsi d'informazione secondo gli artt. 36 e 37 del d. lgs 81/2008 denominato "CORSI NEOASSUNTI".

Registrazione dell'attività: in ogni sito è archiviata tutta la documentazione relativa agli adempimenti sulla sicurezza.

Tutte le funzioni coinvolte nella gestione della sicurezza in azienda (Datore di Lavoro, Dirigenti, Preposti, Medico Competente, Infermeria, RSPP, RLS, ASPP aziendali), compreso tutti i dipendenti che utilizzano il sistema informatico, possono accedere alla intranet aziendale nella quale è possibile trovare e scaricare la documentazione sempre aggiornata relativa ad informazioni / comunicazioni varie, politica aziendale, rapporti e statistiche, principali normative in vigore, manuali e procedure, schede di sicurezza prodotti.

Rapporti con gli enti di controllo: i rapporti con gli enti di controllo sulla sicurezza (a titolo esemplificativo e non esaustivo ASL, ARPA, Vigili del Fuoco, INAIL, Direzione Provinciale del Lavoro, Camera di Commercio etc.) sono gestiti secondo i principi previsti nella Parte Speciale A.

Sistema disciplinare: in caso di violazione dei principi e delle procedure previste a tutela della sicurezza e dell'igiene dei luoghi di lavoro, sono applicate, commisurate alla gravità della violazione, le sanzioni previste dal Capitolo 8 del presente Modello.

L'applicazione delle suddette sanzioni è indipendente dall'eventuale apertura e svolgimento di un procedimento penale.

Outsourcing: nel caso di consulenza esterna, l'accordo dovrà prevedere l'apposita clausola di cui al paragrafo A.3 del presente Modello.

Il pagamento della parcella del professionista esterno è subordinato al controllo sull'effettiva attività svolta e sulla congruità del prezzo rispetto all'attività prestata.

D 4. COMPITI DELL'ORGANISMO DI VIGILANZA

Compiti specifici dell'O.d.V., oltre a quanto previsto precedentemente, sono i seguenti:

- coordinarsi con i responsabili per la sicurezza (in particolare RSPP, ASPP) affinché i controlli ai sensi del d. lgs n. 231/01 siano correttamente integrati con i controlli predisposti ai sensi del d. lgs n. 81/2008 e della normativa vigente sull'igiene e sicurezza del lavoro;
- verificare periodicamente l'osservanza da parte dei Destinatari del Modello dei principi in materia di sicurezza e igiene;
- verificare l'effettiva attuazione dell'impianto sanzionatorio in caso vengano accertate violazioni delle prescrizioni.

Nell'espletamento dei suddetti compiti, l'Organismo di Vigilanza ha libero accesso a tutta la documentazione relativa ai processi sensibili della Parte Speciale "D".

PARTE SPECIALE "E" -

Reati contro la personalità individuale

(art. 25-quinquies)

I reati contro la personalità individuale, contemplati dall'art. 25 quinquies del Dlgs. 231/01, sono perseguibili in base alla normativa vigente in materia di lavoro. Inoltre, comportamenti di qualunque genere lesivi della dignità della persona non sono ammessi dal Codice Etico di Innovhub SSI.

E 1 TIPOLOGIA DEI REATI

Per quanto concerne la presente sezione della Parte Speciale, si citano di seguito le singole fattispecie contemplate nel D.Lgs. 231/2001 all'art. 25 quinquies:

- **Riduzione o mantenimento in schiavitù o in servitù (art. 600 cod. pen.)**

- **Prostituzione Minorile (art. 600-bis c.p.)**
- **Pornografia minorile (art. 600-ter cod. pen.)**
- **Detenzione di materiale pornografico (art. 600-quater cod. pen.)**
- **Iniziative turistiche volte allo sfruttamento della prostituzione minorile (art. 600-quinquies cod. pen.)**
- **Intermediazione illecita o sfruttamento del lavoro (art. 603 bis cp)**

E 2 AREE DI RISCHIO

Le aree di attività ritenute maggiormente a rischio in relazione ai reati contro la personalità individuale sono considerate le seguenti:

- Utilizzo di Internet;
- Trasferte all'estero del proprio personale;

E 3 PRINCIPI DI COMPORTAMENTO

Si prevede l'espresso divieto a carico dei Destinatari di:

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

Si indicano di seguito i principi di comportamento che, in relazione all'area di rischio individuata, i Destinatari sono tenuti a rispettare e che, ove necessario, devono essere implementati in specifiche procedure aziendali ovvero possono formare oggetto di comunicazione da parte del O.d.V. In particolare:

- L'Azienda è tenuta a dotarsi di strumenti informatici costantemente aggiornati al fine di contrastare l'accesso a siti Internet contenenti materiale relativo alla pornografia minorile (strumenti di "content filtering");

- Innovhub SSI richiama in modo inequivocabile i Destinatari a un corretto utilizzo degli strumenti informatici in proprio possesso;

- Nel rispetto delle normative vigenti, l'Azienda si riserva il diritto di effettuare periodici controlli idonei ad impedire l'abuso dei sistemi informativi aziendali o la commissione di Reati attraverso il loro utilizzo;

- Innovhub SSI sanziona inderogabilmente, attraverso il Codice Etico, ogni comportamento lesivo della dignità umana.

PARTE SPECIALE "F" -

Reati di riciclaggio e impiego di denaro, beni o utilità di provenienza illecita

(art. 25-octies)

F 1 TIPOLOGIA DEI REATI

Per quanto concerne la presente sezione della Parte Speciale, si riportano i reati contemplati nell'art. 25-octies del Decreto:

- **Ricettazione (art. 648 c.p.)**
- **Riciclaggio (art. 648 bis c.p.)**
- **Impiego di denaro, beni o utilità di provenienza illecita (art. 648 ter c.p.)**
- **Autoriciclaggio (art. 648 ter, 1 c.p.)**

F 2 AREE DI RISCHIO

L'area di attività ritenuta maggiormente a rischio in relazione ai reati di riciclaggio e impiego di denaro, beni o utilità di provenienza illecita.

F 3 PRINCIPI DI COMPORTAMENTO

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

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

Si indicano di seguito i principi di comportamento che in relazione all'area di rischio individuata i Destinatari sono tenuti a rispettare e che, ove opportuno, devono essere implementati in specifiche procedure aziendali ovvero possono formare oggetto di comunicazione da parte del O.d.V. In particolare:

- Innovhub SSI vieta l'utilizzo del contante o altro strumento finanziario al portatore, per qualunque operazione di incasso, pagamento, trasferimento fondi, impiego o altro utilizzo di disponibilità finanziarie quando il valore dell'operazione, anche frazionata, è complessivamente pari o superiore a 10.000 euro, nonché il divieto di utilizzo di conti correnti o libretti di risparmio in forma anonima o con intestazione fittizia;

- Innovhub SSI impone ai Destinatari l'obbligo di:

- utilizzare operatori finanziari abilitati per la realizzazione di ciascuna delle operazioni di cui alla precedente lettera a);
- utilizzare esclusivamente, nell'ambito della gestione delle transazioni finanziarie, operatori che attestino di essere muniti di presidi manuali e informatici e/o telematici atti a prevenire fenomeni di riciclaggio.

PARTE SPECIALE "G" –

Reati in materia di violazione del diritto d'autore (art. 25-novies)

G. 1 TIPOLOGIA DEI REATI

Di seguito si riportano i reati contemplati nell'art. 25-novies del Decreto:

- Delitti in materia di violazione del diritto d'autore (art. 25-novies, d. lgs. n. 231/2001)
- Messa a disposizione del pubblico in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, e senza averne diritto di un'opera o di parte di un'opera dell'ingegno protetta (art. 171, co. 1, lett a-bis) L. 633/1941)
- Reato di cui al punto precedente commesso su un'opera altrui non destinata alla pubblicità, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera stessa, qualora ne risulti offeso l'onore o la reputazione dell'autore (art. 171, co. 3, L. 633/1941)
- Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita, detenzione a scopo commerciale o imprenditoriale ovvero concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi di protezione di programmi per elaboratori (art. 171-bis, co. 1, L. 633/1941)
- Riproduzione su supporti non contrassegnati SIAE, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati al fine di trarne profitto; estrazione o reimpiego della banca dati in violazione delle disposizioni sui diritti del costitutore e dell'utente di una banca dati; distribuzione, vendita o concessione in locazione di banche di dati (art. 171-bis co. 2, L. 633/1941)
- Reati commessi a fini di lucro, per uso non personale, e caratterizzati da una delle seguenti condotte descritte all'art. 171-ter, comma 1, L. 633/1941:
- Reati caratterizzati da una delle condotte descritte all'art. 171-ter, comma 2, L. 633/1941

G. 2 AREE DI RISCHIO

L'area di attività ritenuta maggiormente a rischio in relazione ai reati in materia di violazione del diritto d'autore sono quelle dei sistemi informatici e della eventuale attività didattica, di formazione e pubblicazioni.

G. 3 PRINCIPI DI COMPORTAMENTO

Si indicano di seguito i principi di comportamento che in relazione all'area di rischio individuata i Destinatari sono tenuti a rispettare e che, ove opportuno, devono essere implementati in specifiche procedure aziendali ovvero possono formare oggetto di comunicazione da parte del O.d.V. In particolare è indispensabile:

- che tutte le attività svolte siano improntate al massimo rispetto delle leggi vigenti, nonché dei principi di correttezza, trasparenza, buona fede e tracciabilità della documentazione;
- i collaboratori esterni siano informati e responsabilizzati in merito al compimento dello specifico reato;
- siano tenuti inventari delle licenze software
- che sia rispettato il principio separazione delle attività (autorizzazione, esecuzione e controllo)

Inoltre, Innovhub SSI vieta a tutti i collaboratori di:

- porre in essere, collaborare o dare causa alla realizzazione dei comportamenti tali da integrare le fattispecie di delitti relativi al diritto d'autore sopra richiamati;
- porre in essere, collaborare o dare causa alla realizzazione di comportamenti, i quali, sebbene risultino tali da non costituire di per sé reato, possano potenzialmente diventarlo.

PARTE SPECIALE "H" -
Reati in materia ambientale

(art. 25 – undecies)

H. 1 TIPOLOGIA DEI REATI

Per quanto concerne la presente sezione della Parte Speciale, si riportano i reati contemplati nell'art. 25-undecies del Decreto:

- **Sanzioni in tema di tutela dei corpi idrici e degli scarichi (art. 137 D. Lgs. 152/06);**
- **Attività di gestione di rifiuti non autorizzata (art. 256 D. Lgs. 152/06);**
- **Violazioni in materia di bonifica dei siti (art. 257 D. Lgs. 152/06);**
- **Violazioni in tema di comunicazione, registri e formulari ambientali (art. 258 D. Lgs. 152/06);**
- **Traffico illecito di rifiuti (art. 259 D. Lgs. 152/06);**
- **Attività organizzate per il traffico illecito di rifiuti (art. 260 D. Lgs. 152/06);**
- **Violazioni in relazione al Sistema «SISTRI» (art. 260 bis D. Lgs. 152/06);**
- **Sanzioni in tema di prevenzione e limitazione delle emissioni atmosferiche (art. 279 D. Lgs. 152/06);**

- **Impiego di sostanze lesive dell'ozono e dell'ambiente (art. 3 L. 28 dicembre 549/93);**
- **Uccisione, distruzione, cattura, prelievo, detenzione di esemplari di specie animali o vegetali selvatiche protette (art. 727-bis C.P.);**
- **Distruzione o deterioramento di habitat all'interno di un sito protetto (art. 333-bis C.P.);**

H. 2 AREE DI RISCHIO

Le aree di attività ritenute maggiormente a rischio in relazione ai reati in materia ambientale sono quelle della gestione dei rifiuti e di qualsivoglia attività ad essa collegata, anche svolta da o per soggetti terzi.

H. 3 PRINCIPI DI COMPORTAMENTO

Si indicano di seguito i principi di comportamento che in relazione all'area di rischio individuata i Destinatari sono tenuti a rispettare e che, ove opportuno, devono essere implementati in specifiche procedure interne ovvero possono formare oggetto di comunicazione da parte del O.d.V. In termini generali:

- che tutte le attività svolte siano improntate al massimo rispetto delle leggi vigenti, nonché dei principi di correttezza, trasparenza, buona fede e tracciabilità della documentazione;
- i collaboratori esterni siano informati e responsabilizzati in merito alla commissione dello specifico reato;
- che sia rispettato il principio di separazione delle attività (autorizzazione, esecuzione e controllo)

Inoltre, Innovhub SSI vieta a tutti i collaboratori di:

- porre in essere, collaborare o dare causa alla realizzazione dei comportamenti tali da integrare le fattispecie dei reati ambientali;
- porre in essere, collaborare o dare causa alla realizzazione di comportamenti, i quali, sebbene risultino tali da non costituire di per sé reato, possano potenzialmente diventarlo.

Inoltre, in particolare:

- Innovhub SSI garantisce che lo smaltimento e lo stoccaggio dei rifiuti avvenga secondo le vigenti discipline in materia. Per quanto attiene ai rifiuti urbani o assimilabili che vengono prodotti internamente, in attesa di essere smaltiti con le modalità di cui sopra, essi sono raccolti in modo separato e temporaneamente depositati in apposite aree a seconda del genere e del tipo di rifiuto.
- Misure di sicurezza - lo standard richiede che la gestione dei rifiuti (sia speciali che urbani che assimilabili ad urbani) sia gestita in conformità alla normativa vigente.

– Tracciabilità: lo standard richiede che siano tracciate le attività di conferimento di rifiuti speciali (toner esausti) a ditta autorizzata e che siano gestite le registrazioni afferenti.

PARTE SPECIALE "I" -
Processi strumentali

I. 1 TIPOLOGIA DEI REATI

Sono stati oggetto d'analisi alcuni processi che potrebbero essere considerati "strumentali" alla commissione dei c.d. "reati presupposto".

Qui di seguito sono elencati i processi strumentali identificati.

1. **Gestione dei flussi finanziari:** l'attività si riferisce alla gestione ed alla movimentazione delle risorse finanziarie relative all'attività di impresa.

2. **Assegnazione e gestione di incarichi per servizi e consulenza:** si tratta dell'attività di gestione in generale del processo di procurement relativamente a servizi professionali (quali, ad esempio, ingegneri, architetti, professori universitari, avvocati etc.).

3. **Selezione e gestione degli intermediari/partner/ fornitori:** si tratta della gestione in generale dei rapporti con soggetti terzi con i quali si sviluppano forme di collaborazione contrattualmente definite. Tale attività include la collaborazione che Innovhub SSI presta a favore di clienti privati nell'ambito di contratti di project development. Tali contratti possono, infatti, prevedere il contributo di Innovhub SSI nella selezione e la gestione di partner/fornitori/appaltatori/consulenti.

4. **Gestione delle assunzioni e del sistema premiante:** si tratta dell'attività relativa al processo di selezione, assunzione, retribuzione e valutazione e dei meccanismi di incentivazione del personale.

5. **Gestione omaggi,** nonché spese di rappresentanza: si tratta delle attività di gestione degli omaggi e pubblicitarie (es: borse di studio, inviti a congressi, visite a siti, partecipazione a fiere, congressi, pubblicazioni scientifiche, etc.) nonché dell'attività di gestione delle spese di rappresentanza.

6. **Gestione di atti di liberalità:** si tratta della gestione delle attività relative alle donazioni e, in generale, agli atti di liberalità.

7. Obblighi previdenziali: si tratta della gestione delle attività volte al rispetto degli adempimenti di legge relativi ai trattamenti previdenziali del personale dipendente, dei collaboratori e la relativa disciplina sanzionatoria.

8. Gestione del sistema informativo: l'attività è quella relativa alla gestione del sistema informativo aziendale e dei relativi sistemi di controllo.

9. Abbandono dei rifiuti: l'attività è quella relativa all'abbandono dei rifiuti come previsto dall'art. 192 del D.lgs n. 152/2006

I. 2 AREE DI RISCHIO

Tutte le aree di attività sono potenzialmente ritenute a rischio in relazione alla possibile commissione di reati connessi ai processi strumentali.

I. 3 PRINCIPI

Il sistema dei controlli, perfezionato dall'Azienda anche sulla base delle indicazioni fornite dalle Linee guida elaborate dalle principali Associazioni di categoria, dalla Regione Lombardia e dalle best practice internazionali in tema di rischi di frode e corruzione, prevede con riferimento ai processi strumentali individuati:

- principi generali degli standard di controllo;
- standard di controllo "specifici" applicati ai singoli processi strumentali.

I.3.1 Principi generali degli standard di controllo relativi ai processi strumentali

Gli standard di controllo sono fondati sui seguenti principi generali:

- Segregazione dei compiti: gli standard si fondano sulla separazione delle attività tra chi autorizza, chi esegue e chi controlla.
- Esistenza di disposizioni aziendali/procedure formalizzate: gli standard si fondano sull'esistenza di disposizioni aziendali e/o di procedure formalizzate idonee a fornire principi di comportamento, modalità operative per lo svolgimento delle attività sensibili nonché modalità di archiviazione della documentazione rilevante.
- Poteri autorizzativi e di firma: gli standard si fondano sul principio secondo il quale i poteri autorizzativi e di firma devono essere: i) coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, indicazione delle soglie di approvazione delle spese; ii) chiaramente definiti e conosciuti all'interno dell'Azienda.
- Tracciabilità: gli standard si fondano sul principio secondo cui: i) ogni operazione relativa all'attività sensibile sia, ove possibile, adeguatamente registrata; ii) il processo di decisione, autorizzazione e svolgimento dell'attività sensibile sia verificabile ex post, anche tramite appositi supporti documentali; iii) in ogni caso, sia disciplinata in dettaglio la possibilità di cancellare o distruggere le registrazioni effettuate.

I.3.2 Standard di controllo specifici

Qui di seguito sono elencati gli standard di controllo specifici relativi ai processi strumentali sopra individuati.

1 Gestione dei flussi finanziari:

- Disposizioni aziendali: lo standard concerne la formalizzazione di una disposizione aziendale per la gestione dei flussi finanziari che definisca, fra l'altro: i) ruoli e responsabilità dei soggetti coinvolti; ii) pianificazione dei budget di spesa di ciascuna funzione; iii) tipologie di transazioni eseguibili direttamente dalle varie funzioni aziendali; iv) controlli specifici e preventivi da applicarsi in casi, tassativamente previsti, in deroga alla normale procedura (es. pagamenti urgenti); v) regole per la gestione dei flussi finanziari che non rientrino nei processi tipici aziendali e che presentino caratteri di estemporaneità e discrezionalità.
- Registrazione: ogni operazione che comporta l'utilizzo o impiego di risorse economiche o finanziarie ha una causale espressa ed è documentata e registrata in conformità ai principi di correttezza professionale e contabile.
- Autorizzazione formale: lo standard richiede un'autorizzazione formalizzata alla disposizione di pagamento, con limiti di spesa, vincoli e responsabilità e la specificazione della motivazione relativa alla spesa stessa.
- Documentazione: l'impiego di risorse finanziarie è motivato, con documenti giustificativi, attestazione di inerenza e congruità, inviati ed approvati dal superiore gerarchico nonché archiviati.
- Pagamenti: lo standard richiede: i) al momento del pagamento del corrispettivo, una valutazione di congruità del corrispettivo con riferimento a contratto / fattura; ii) che nessun pagamento in favore di fornitori sia effettuato in contanti o per mezzo di titoli al portatore e effettuato a soggetto diverso o in luogo/Paese diverso da quello in cui il fornitore ha reso la propria attività, salvo specifiche eccezioni opportunamente motivabili.

2 Assegnazione e gestione di incarichi per servizi e consulenza:

- Disposizione aziendale: lo standard concerne la formalizzazione di una disposizione aziendale con previsione, fra l'altro di: i) criteri oggettivi e trasparenti per la selezione dei consulenti e dei professionisti esterni (ad esempio, capacità tecnica, esperienza, referenze qualificanti, politica di prezzo etc.) che collaborino con l'Azienda, salvo specifiche consulenze direzionali. L'elenco di tali consulenze direzionali, con relative motivazioni, sarà inviato con cadenza annuale all'Organismo di Vigilanza; ii) separazione di funzioni tra coloro che selezionano i consulenti e coloro che ne controllano l'operato.
- Documentazione: lo standard concerne la predisposizione e l'archiviazione di documenti giustificativi degli incarichi conferiti, con motivazione e attestazione di inerenza e congruità, approvati da adeguato livello gerarchico.
- Pagamenti: lo standard richiede: i) al momento del pagamento del corrispettivo, una valutazione di congruità del corrispettivo con riferimento al contratto / alla prestazione resa / alla fattura con un visto per approvazione del pagamento da parte della funzione coinvolta; ii) che nessun pagamento in favore del consulente sia effettuato in contanti o per mezzo di titoli al portatore e effettuato a soggetto diverso dal consulente o in luogo/Paese diverso da quello in cui il consulente ha reso i propri servizi, salvo specifiche eccezioni opportunamente motivabili.

- Contratti: lo standard concerne: i) l'obbligo di formalizzare e sottoscrivere i contratti di consulenza/collaborazione prima dell'inizio della prestazione e la limitazione a casi eccezionali, specificamente motivati per iscritto, della possibilità di concludere contratti successivamente all'inizio della prestazione; ii) la previsione, nei contratti di consulenza per soggetti che collaborano con l'Azienda, di specifiche clausole con cui i consulenti dichiarino di conoscere e si obblighino a rispettare le previsioni del Modello Organizzativo e i principi etici contenuti nel Codice etico nonché di clausole risolutive espresse che attribuiscano a Innovhub SSI la facoltà di risolvere i contratti in questione in caso di violazione di tale obbligo.
- Codice etico: lo standard richiede l'esplicita previsione tra i principi etici del divieto di pratiche corruttive.

3 Selezione e gestione degli intermediari/partner /fornitori:

- Disposizione aziendale: lo standard richiede la formalizzazione di una disposizione aziendale per la gestione dei rapporti con soggetti ai quali Innovhub SSI abbia conferito uno specifico incarico e con i partner (nel caso ad esempio di ATI, ATS) con previsione, fra l'altro, di criteri oggettivi e trasparenti per la selezione con riferimento a requisiti non solo di solidità patrimoniale e capacità tecnica, ma anche di onorabilità e integrità. Nel caso di stipulazione di accordi (ATI, ATS, ecc.), è necessaria una chiara attribuzione dei ruoli, delle responsabilità, dei costi e degli utili tra i partner. I criteri per la selezione e la gestione dei rapporti con tali soggetti terzi sono applicati anche nel caso in cui Innovhub SSI svolga tali attività nell'ambito di rapporti contrattuali con soggetti privati.

- Contratti: lo standard richiede che i contratti con soggetti che operino per la Società o collaborino con la Società nello svolgimento di attività nelle aree "sensibili" prevedano, salvo specifiche eccezioni opportunamente motivabili: i) specifici richiami al rispetto dei principi etici contenuti nel Codice Etico e delle disposizioni del Modello Organizzativo ; ii) clausole risolutive espresse che attribuiscano a Innovhub SSI la facoltà di risolvere i contratti in questione in caso di violazione di tale obbligo; iii) un preciso impegno da parte della controparte contrattuale a dotarsi di misure idonee a prevenire il rischio di commissione dei reati richiamati dal d.lgs. n. 231/2001 che potrebbero essere ascritti alla Società;
- Codice Etico: lo standard richiede l'osservanza delle regole comportamentali previste in tema di divieto di pratiche corruttive.

4 Gestione delle assunzioni e del sistema premiante:

- Disposizioni aziendali: lo standard concerne la formalizzazione di una disposizione aziendale per l'assunzione del personale con previsione, fra l'altro, di quanto di seguito indicato: i) criteri di selezione dei candidati oggettivi e trasparenti (ad esempio, voto di laurea/diploma, conoscenza di lingue straniere, precedenti esperienze professionali, ecc.); ii) definizione di ruoli e responsabilità dei soggetti coinvolti con intervento di due soggetti nella selezione del candidato e nella valutazione/promozione del dipendente; iii) modalità di archiviazione della documentazione rilevante.

- Documentazione: lo standard richiede che il processo di selezione/assunzione/promozione sia adeguatamente documentato e che la documentazione sia conservata in apposito archivio.
- Obiettivi di performance: lo standard concerne la definizione di sistemi premianti che includano obiettivi predeterminati, misurabili e realistici, nonché l'intervento di più funzioni nella definizione dei piani di incentivazione e nella selezione dei relativi beneficiari.

5 Gestione omaggi nonché spese di rappresentanza:

- Disposizioni aziendali: lo standard concerne la formalizzazione di una disposizione aziendale per la gestione degli omaggi e spese di rappresentanza con previsione, fra l'altro, di quanto di seguito indicato: i) definizione di ruoli/responsabilità dei soggetti coinvolti; ii) indicazione di limiti di valore degli omaggi e delle spese di rappresentanza; iii) criteri di selezione che regolano in maniera chiara e precisa l'individuazione delle iniziative finanziate; iv) conservazione della documentazione rilevante.
- Autorizzazione formale: lo standard richiede l'esistenza di un'autorizzazione formalizzata ad effettuare omaggi.
- Elenco dei beneficiari di omaggi: lo standard richiede la redazione un elenco dei soggetti cui vengono inviati omaggi o a favore dei quali vengono sostenute spese di rappresentanza per un valore superiore ai 300 euro, con specifica indicazione dei soggetti riconducibili alla P.A. e dell'omaggio o spesa di rappresentanza relativi a ciascun beneficiario.
- Codice Etico: lo standard richiede l'osservanza delle regole comportamentali previste dal Codice Etico in tema di divieto di pratiche corruttive.

6 Gestione di donazioni e atti di liberalità

- Criteri di selezione: ove previsti, devono esistere criteri di selezione che regolano, in maniera chiara e precisa, la scelta delle Associazioni/Fondazioni in favore delle quali effettuare donazioni od erogazioni liberali di qualsiasi tipo e l'individuazione delle iniziative finanziate.
- Lista: deve essere redatta una lista dei beneficiari abituali/ricorrenti di donazioni e/o erogazioni liberali di qualsiasi tipo. Le modalità di inserimento, mantenimento ed eliminazione dei beneficiari dovranno essere debitamente formalizzate.
- Autorizzazione: le donazioni e le erogazioni liberali di qualsiasi tipo devono essere adeguatamente autorizzate, formalizzate e rendicontate.
- Versamenti: le donazioni e le erogazioni liberali di qualsiasi tipo non possono essere effettuate tramite versamenti in contanti o su conti correnti cifrati.
- Documentazione: l'impiego di risorse finanziarie è motivato con documenti giustificativi debitamente archiviati.

7 Obblighi previdenziali.

- Verifica: della conformità tra i dati forniti dai sistemi di amministrazione del personale e quelli dichiarati agli organi competenti
- Tracciabilità: degli atti e delle fonti informative delle singole attività di processo

8 Gestione del sistema informatico.

- Misure di sicurezza: lo standard impone la necessaria esistenza di adeguate misure di sicurezza per il trattamento informatico dei dati, quali quelle contenute nel d.lgs. n. 196/03, come modificato ex L. 167/2017 che ha recepito i Regolamenti UE 679/2016 e 680/2016 in vigore dal maggio 2018, e nelle best practice internazionali.
- Tracciabilità: lo standard richiede l'esistenza di presidi che, in relazione ad ogni comunicazione scritta relativa a ciascuna attività sensibile, assicurino la tracciabilità degli elementi informativi e delle relative fonti. Lo scambio di comunicazioni, informazioni e autorizzazioni tra i soggetti coinvolti nei rispettivi processi è soggetto ad obblighi di conservazione in appositi e sicuri archivi non accessibili a terzi. Particolare attenzione deve essere prestata anche nel caso di utilizzo di sistemi informatici per lo scambio di informazioni (e-mail e documenti elettronici devono essere conservati in appositi spazi elettronici non accessibili a terzi e protetti da adeguati sistemi di password).
- Modifica dei dati: il controllo richiede l'affidamento esclusivo al servizio competente, che deve assicurare la tracciabilità della modifica di dati, liste di controllo e archivi.
- Liste di controllo e segnalazioni automatiche: è prevista l'esistenza di liste di controllo degli accessi ai sistemi informativi e automatismi di segnalazione all'amministratore del sistema di operazioni non autorizzate, quali a titolo esemplificativo, cancellazioni, tentativi di accesso, alterazione delle funzionalità del sistema, ecc.

9 Impiego di cittadini extracomunitari il cui soggiorno è irregolare

Disposizioni: qualora venisse coinvolto come collaboratore di Innovhub SSI un cittadino proveniente da un paese extra UE, l'Azienda garantisce che preventivamente sia richiesto il permesso di soggiorno e di assicurarsi della validità dello stesso.

I soggetti che operano in collaborazione con Innovhub SSI in modo abituale per lo svolgimento dei servizi generali (es. pulizie, ecc.) vengono incaricati a seguito di procedura di gara indetta dalla Camera di Commercio che esegue i controlli necessari.

Misure di sicurezza: lo standard richiede che venga data dimostrazione del regolare impiego di cittadini provenienti da Paesi extra UE (sia coinvolti direttamente sia tramite i fornitori).

Tracciabilità: lo standard richiede che eventuale documentazione afferente il possesso di regolare permesso di soggiorno e le dichiarazioni dei fornitori sia disponibile per i controlli.

10 Razzismo e xenofobia

Disposizioni: qualsiasi forma di propaganda di razzismo, xenofobia anche mediante istigazione al razzismo o alla xenofobia posta in essere da dipendenti o collaboratori.

Misure di sicurezza: formazione