

POLICY ANTIFRODE
GRUPPO SNAITECH

Aprile 2025

1.	SNAITECH S.P.A. E LE SOCIETÀ DEL GRUPPO SNAITECH.....	3
2.	SCOPO E AMBITO DI APPLICAZIONE DELLA POLICY ANTIFRODE.....	4
3.	DEFINIZIONI.....	6
4.	PRINCIPI GENERALI.....	7
5.	IL CONCETTO DI FRODE.....	8
6.	LA PREVENZIONE E IL CONTRASTO DELLE FRODI NELL'AMBITO DEL GRUPPO SNAITECH.....	10
6.1.	GOVERNANCE DEL RISCHIO FRODE.....	10
6.2.	SISTEMA SANZIONATORIO.....	10
7.	PROCESSO DI PREVENZIONE E MONITORAGGIO DEL RISCHIO FRODE.....	12
7.1.	PROCESSI AZIENDALI E VALUTAZIONE DEL RISCHIO FRODE.....	12
7.2.	ATTIVITÀ DI CONTROLLO.....	12
7.3.	ATTIVITÀ DI MONITORAGGIO.....	13
8.	CANALI DI SEGNALAZIONE.....	14
8.1.	MODALITÀ DI SEGNALAZIONE.....	14
9.	SVOLGIMENTO DELLE INDAGINI.....	15
10.	DOVERI DI FORMAZIONE.....	16
10.1	EROGAZIONE DELLA FORMAZIONE AL PERSONALE.....	16
10.2	LA PREVENZIONE DEI FENOMENI FRAUDOLENTI NEI RAPPORTI ESTERNI.....	16

1. SNAITECH S.p.A. E LE SOCIETÀ DEL GRUPPO SNAITECH

SNAITECH S.p.A. è uno dei principali Concessionari per la gestione dei giochi autorizzati in Italia: offre, tramite la rete fisica e online, scommesse su eventi sportivi e non, scommesse ippiche, concorsi a pronostico, scommesse su eventi virtuali, *videolottery*, *new slot* ed esclusivamente online *casinò games*, *slot online*, *skill games* e bingo.

SNAITECH S.p.A., al contempo, agisce quale vertice di un Gruppo di società controllate che operano nello stesso settore del gioco lecito, seppure con funzioni e attraverso attività differenti rispetto a quelle della capogruppo, integrando e completando i servizi offerti attraverso il coordinamento di una rete retail attiva su tutto il territorio nazionale, la gestione di piattaforme proprietarie (compresi canali televisivi satellitari) e degli ippodromi di Milano e Montecatini Terme.

Del Gruppo fa anche parte la Fondazione Snaitech - Ente Filantropico ETS - che, in quanto ente autonomo senza scopo di lucro, persegue esclusivamente finalità di solidarietà sociale nei campi della sanità, dell'assistenza sociale e della beneficenza, dell'istruzione e formazione, della promozione della cultura, dell'arte e della ricerca scientifica e che attengono alla tutela dei diritti civili al servizio di collettività meno abbienti.

2. SCOPO E AMBITO DI APPLICAZIONE DELLA POLICY ANTIFRODE

Il Gruppo SNAITECH persegue i valori dell'onestà e della legalità, facendo riferimento non soltanto alla normativa nazionale, ma anche alla legislazione vigente in ciascun Paese in cui si trovi ad operare, alle normative dell'UE, nonché ad ogni principio o convenzione internazionale applicabile per il proprio settore di riferimento.

La presente *policy* definisce i principi generali e le regole di condotta in materia di prevenzione e contrasto delle frodi che devono essere rispettati nell'ambito del Gruppo SNAITECH.

Ciascuna società del Gruppo SNAITECH adotta la presente *policy* e si conforma ai principi e alle regole di comportamento dalla stessa stabilite.

Obiettivo della presente *policy* è promuovere all'interno di SNAITECH S.p.A., nonché delle altre Società che compongono il Gruppo SNAITECH, l'integrità dei comportamenti dei dipendenti e del *management*, e ciò nella convinzione che i soggetti economici non possano avere una buona condotta senza il rispetto dei principi etici. In tale contesto, infatti, ogni Società del Gruppo SNAITECH è tenuta ad operare in piena legalità e rispettando le regole e i principi di comportamento definiti all'interno del già adottato Codice Etico di Gruppo.

Al fine di proseguire il processo di rafforzamento e miglioramento continuo del proprio sistema di *governance* in un'ottica di consolidamento del modello di conduzione responsabile della propria attività, il Gruppo SNAITECH ha deciso di adottare la presente *Policy Antifrode* finalizzata a delineare il proprio modello di governo e controllo del rischio frode.

In particolare, la *policy* Antifrode mira a definire:

- i ruoli e le responsabilità;
- il processo di prevenzione e monitoraggio del rischio frode;
- il sistema disciplinare;
- i canali di segnalazione;
- il processo investigativo.

L'ambito di applicazione della presente *policy* si estende a tutte le società che costituiscono il Gruppo SNAITECH, ovvero:

- SNAITECH S.p.A.;
- ciascuna delle società controllate da SNAITECH S.p.A.;
- Fondazione Snaitech – Ente Filantropico ETS.

Sono destinatari della presente *policy* tutti coloro che – a vario titolo – prestano la propria attività nell'interesse di SNAITECH S.p.A., di ciascuna delle società dalla stessa controllate o dell'intero Gruppo SNAITECH (componenti degli organi amministrativi, di vigilanza e di controllo, dirigenti, dipendenti, collaboratori a qualunque titolo, consulenti, partner, fornitori, etc.).

I contenuti della *policy* sono da intendersi integrativi rispetto agli strumenti normativi esistenti costituiti:

- dal Codice Etico del Gruppo SNAITECH, che raccoglie e definisce il complesso dei valori e dei principi di comportamento che devono improntare l'operato dell'intero Gruppo SNAITECH e di ciascuna delle società che lo compongono;

- dal Modello di Organizzazione, Gestione e Controllo *ex* D.Lgs. n. 231/01 adottato da ciascuna Società del Gruppo SNAITECH;
- dalla *policy* Anticorruzione del Gruppo SNAITECH;
- dalle procedure, dalle linee guida e dai manuali operativi adottati internamente da ciascuna società per disciplinare lo svolgimento della propria attività.

3. DEFINIZIONI

Ai fini della presente *policy*, i termini elencati assumono il significato di seguito specificato:

SNAITECH: la società SNAITECH S.p.A.;

Gruppo SNAITECH (o Gruppo): il gruppo di società facenti capo a SNAITECH S.p.A.;

Società controllate (o Controllate): le Società in controllo, diretto o indiretto, di SNAITECH S.p.A.;

Codice Etico: Codice Etico del Gruppo SNAITECH;

Destinatari: il personale di SNAITECH S.p.A. e delle società controllate (componenti degli organi amministrativi, di vigilanza e di controllo, dirigenti, dipendenti) nonché chiunque, a qualsiasi titolo, presti attività lavorativa in favore del Gruppo o di una o più delle società che lo compongono (es. consulenti, collaboratori esterni, partner, fornitori, etc.);

Frode o pratica fraudolenta: ogni attività ingannevole o intenzionalmente fuorviante realizzata al fine di confondere o ingannare una parte, per ottenerne un beneficio finanziario o di altro tipo, oppure per evitare un obbligo, a proprio vantaggio o di altri;

ACFE Fraud Tree: modello per l'esemplificazione dei possibili schemi di frode, classificati in tre macro-categorie (corruzione, appropriazione indebita e frodi di bilancio), elaborato dall'*Association of Certified Fraud Examiners*;

Normativa Antifrode: la normativa nazionale ed internazionale applicabile in Italia e nei Paesi all'interno dei quali il Gruppo SNAITECH opera;

Segnalazione: l'attività di *report* attraverso la quale vengono segnalati fenomeni di frode che coinvolgono l'attività del Gruppo SNAITECH, delle società che lo compongono, oppure di uno o più soggetti che, a qualunque titolo, prestano attività nell'interesse dello stesso Gruppo o di ciascuna delle società appartenente allo stesso;

Segnalante: qualsiasi soggetto (interno ed esterno al Gruppo SNAITECH) che effettua una Segnalazione;

Segnalato: qualsiasi soggetto a cui sono riferiti o riferibili i fatti oggetto di una segnalazione;

Direzione Affari Legali e Societari (o Direzione Legale): la Direzione che ha il compito di ricevere, analizzare e gestire le segnalazioni in materia di frode fatta eccezione per quelle rientranti nell'ambito di applicazione del D.Lgs. n. 24/2023 (Decreto *Whistleblowing*) che saranno comunicate e gestite dal Comitato *Whistleblowing*;

Comitato Whistleblowing: organismo in forma collegiale, appositamente costituito da membri esperti in materia (interni e/o esterni alle Società del Gruppo SNAITECH), avente il compito di gestire le segnalazioni che rientrano nel perimetro applicativo del D.Lgs. n. 24/2023 (Decreto *Whistleblowing*).

4. PRINCIPI GENERALI

Il complesso dei valori e dei principi etici cui deve conformarsi chiunque, a qualsiasi titolo, presti la propria attività in favore del Gruppo SNAITECH o delle società che ad esso appartengono sono definiti all'interno del Codice Etico del Gruppo SNAITECH.

In ottica di prevenzione delle frodi, si richiede ad ogni Destinatario: *(i)* di agire con integrità nello svolgimento del proprio lavoro, avendo cura che la propria condotta professionale non sia influenzata da possibili guadagni o vantaggi personali; *(ii)* di segnalare tempestivamente qualsiasi episodio dubbio; *(iii)* di utilizzare correttamente gli strumenti, i mezzi economici e le risorse affidate loro a qualunque titolo; *(iv)* di adempiere alle mansioni assegnate con la diligenza, l'accuratezza e la professionalità necessarie.

5. IL CONCETTO DI FRODE

In via generale, il concetto di frode è riconducibile ad ogni attività ingannevole o intenzionalmente fuorviante realizzata al fine di confondere o ingannare una parte, per ottenerne un beneficio finanziario o di altro tipo, oppure per evitare un obbligo, a proprio vantaggio o di altri.

Per quel che interessa le realtà aziendali, il modello ACFE classifica le frodi in tre macrocategorie, ovvero la corruzione, l'appropriazione indebita e le frodi di bilancio.

La presente *policy* mira a disciplinare le condotte di frode riconducibili all'appropriazione indebita, restando invece escluse le condotte riconducibili a schemi corruttivi (per le quali vigono le disposizioni della *policy* Anticorruzione del Gruppo SNAITECH) e le frodi di bilancio (presidiate dalle procedure aziendali nonché dai protocolli individuati nel Modello di Organizzazione, Gestione e Controllo adottato dalle società del Gruppo ex D.Lgs. 231/01).

Le prescrizioni della *policy* si riferiscono a:

- **frodi interne**, ossia comportamenti fraudolenti posti in essere dal personale di SNAITECH S.p.A. e delle controllate, a prescindere dal livello e dall'inquadramento;
- **frodi esterne**, messe in atto da soggetti esterni all'organizzazione aziendale.

Con "frode" si intende qualsiasi comportamento posto in essere da un soggetto che, omettendo, eludendo o trasgredendo norme interne (politiche, procedure, istruzioni operative, ecc.) e/o esterne, procura a sé o ad altri un ingiusto profitto a danno della Società.

A titolo esemplificativo e non esaustivo può rinvenirsi una condotta di frode nel caso di:

- appropriazione indebita di denaro: furti di cassa, sovrapprezzamento attivo, omesso riversamento delle somme dovute al Concessionario, esborsi fraudolenti nei confronti dei dipendenti (falsificazione della retribuzione, rimborsi spese fittizi, ecc.), falsificazione di assegni, sottrazione di fondi prima della loro contabilizzazione (vendite e crediti);
- appropriazione indebita di rimanenze di magazzino e *asset*: uso di beni aziendali a scopo personale, furti, etc.
- nell'ambito del gioco a distanza, la creazione di c.d. *multiple account* (o *chip dumping*): utilizzo di più account contemporaneamente (o collusione tra due o più giocatori online che siedono al medesimo tavolo virtuale l'uno contro l'altro), eventualmente anche mediante l'uso di dispositivi e indirizzi IP diversi per evitare il rilevamento;
- nell'ambito del gioco a distanza, abuso nell'utilizzo dei bonus di gioco, ad esempio mediante la creazione di più account per usufruire dei bonus di ingresso/iscrizione;
- nell'ambito del gioco a distanza, accesso illegittimo a conti di gioco online (*phishing*);
- utilizzo di documenti di identità falsi o oggetto di furto in occasione dell'apertura di conti di gioco;
- utilizzo di dispositivi elettronici illegali (es. *jammer*) in grado di alterare il regolare funzionamento degli apparecchi di gioco;
- manomissione fraudolenta degli apparecchi di gioco, con conseguente alterazione dei flussi, ad esempio mediante le c.d. doppie schede o gli abbattitori;

- apertura di conti di gioco da parte del personale dipendente o di gestori di punti di vendita, in violazione della vigente normativa;
- raccolta illecita di scommesse su eventi sportivi da parte del personale dipendente, al di fuori del sistema di gioco regolamentato.

6.1 Governance del rischio frode

L'**Organo Amministrativo** determina il c.d. “*tone at the top*” in quanto responsabile della promozione di una cultura aziendale improntata a principi di integrità e lealtà. Tale organo garantisce il libero accesso a informazioni e dati utili a valutare, prevenire, intercettare, rilevare anche *ex post* il rischio di accadimento/l'effettivo realizzarsi di eventi di frode alle funzioni interne preposte al monitoraggio e controllo (i.e. al 2° livello di controllo: *Risk Management* e *Compliance* e al 3° livello di controllo *Internal Audit*).

Gli organi di gestione e controllo della Società sono promotori di una politica di prevenzione delle “Frodi” che espletano attraverso la costruzione e il monitoraggio di un Sistema di Controllo Interno e Gestione dei Rischi *che prevede l'applicazione di specifici presidi a mitigazione del rischio frode*.

La **Direzione Legale** è responsabile di valutare le segnalazioni a potenziale rischio frode (ove tale rischio sia collegato a una delle materie/ambiti di segnalazione indicati nella presente *policy*), avviare eventuali investigazioni ed esaminare le risultanze, attivando le strutture/figure aziendali competenti per la definizione delle eventuali azioni correttive/misure disciplinari. Qualora a seguito degli approfondimenti la stessa valuti che la materia oggetto di segnalazione rientri nell'ambito di applicazione del Decreto *Whistleblowing*, procederà ad informare il Comitato *Whistleblowing* entro 7 (sette) giorni dalla data di ricezione della segnalazione al fine della puntuale gestione della stessa. Di detta procedura sarà informato anche il Segnalante, nel totale rispetto della riservatezza della sua identità e del contenuto della segnalazione.

La Direzione Legale è altresì responsabile di predisporre flussi di *reporting* agli Organi di amministrazione e di controllo.

La **Direzione Risorse Umane** contribuisce a favorire la cultura della prevenzione mediante periodiche attività di informazione/formazione sul rischio frode, sui presidi di controllo in essere e sul sistema disciplinare vigente, al fine di sviluppare la consapevolezza nel dipendente di poter incorrere in illeciti passibili di conseguenze disciplinari e/o penalmente rilevanti in caso di comportamenti non conformi al corpo procedurale aziendale, oltre che a leggi e regolamenti.

Il **management** costruisce e sviluppa i processi operativi, individuando i potenziali schemi/scenari di frode applicabili, valutando il rischio frode ed il sistema di controllo interno a presidio del rischio identificato, ponendo in essere le misure correttive (ove necessario), e in generale garantendo l'applicazione dei presidi di controllo definiti.

I **dipendenti**, indipendentemente dal livello e dall'inquadramento, sono tenuti ad operare nel rispetto del corpo procedurale aziendale e di leggi e regolamenti, segnalando ogni eventuale sospetto di condotta fraudolenta.

6.2. Sistema Sanzionatorio

La *policy* Antifrode è adottata da ciascuna società del Gruppo SNAITECH ad integrazione e completamento di quanto previsto dal proprio Modello di Organizzazione, Gestione e Controllo. Per tale ragione, al verificarsi di infrazioni alle disposizioni della presente *policy*, ogni società del Gruppo è tenuta a valutare l'adozione di sanzioni nei confronti degli autori delle stesse, nelle modalità previste dal sistema sanzionatorio definito all'interno del proprio Modello.

Ogni Modello, infatti, definisce un sistema sanzionatorio, rispettoso dei principi di gradualità e proporzionalità della sanzione rispetto alla effettiva gravità del fatto accertato, per mezzo del quale sono previste conseguenze di diversa natura a seconda della tipologia di Destinatario:

- nei confronti del personale dipendente (impiegati, quadri e dirigenti) sono applicabili le sanzioni disciplinari previste dai Contratti Collettivi Nazionali del Lavoro applicabili, quali richiami verbali o scritti, comminazione di multe, sospensione dallo stipendio fino al licenziamento;
- qualora le condotte di frode siano riferibili ad Amministratori, Sindaci o membri degli Organismi di Vigilanza, dovrà esserne data tempestiva notizia all'Organo amministrativo affinché lo stesso possa prendere gli opportuni provvedimenti (es. revoca delle deleghe, decadenza dall'incarico, etc.);
- nei confronti di terzi soggetti contrattualizzati (fornitori, consulenti, procacciatori, etc.) si applicano, se presenti, le clausole contrattuali che indicano gli effetti di atti di frode, anche se solo tentati (es. applicazione di penalità, o risoluzione). In ogni caso, la violazione dei principi generali e delle regole di comportamento costituiscono inadempimento e possono comportare la risoluzione del contratto, eventualmente accompagnata dalla richiesta di risarcimento del danno cagionato alla Società o al Gruppo.

7. PROCESSO DI PREVENZIONE E MONITORAGGIO DEL RISCHIO FRODE

Le attività di seguito descritte attengono al processo di prevenzione e monitoraggio del rischio frode, ponendo l'accento sulla rilevazione e valutazione del rischio, sulle attività di controllo a presidio dello stesso in chiave preventiva e successiva e sulle attività di monitoraggio a tutela dell'intero sistema.

7.1. Processi aziendali e valutazione del rischio "Frode"

I processi aziendali sono costruiti con lo scopo di individuare e valutare *ex ante* l'applicabilità teorica di possibili schemi/scenari di frode riconducibili alle attività operative e alle peculiarità organizzative del Gruppo al fine di orientare misure di prevenzione, controllo e intercettazione del rischio.

La valutazione del rischio frode è demandata ai responsabili di Direzione/Funzione, i quali devono considerare la probabilità di accadimento dell'evento fraudolento, l'impatto dello stesso, i presidi di controllo interno a mitigazione del rischio e le azioni correttive/integrative da porre in essere.

Le Funzioni *Internal Audit*, *Compliance* e *Risk Management* supportano il *management* nell'identificare/confermare i processi aziendali potenzialmente suscettibili di rischio frode rispetto alla previsione di elementi di prevenzione specifica supporto e garanzia del Sistema di Controllo Interno e Gestione dei Rischi in essere.

Le attività sono svolte sulla base delle *best practice* internazionali di riferimento riconducibili alle peculiarità organizzative e di processo del Gruppo.

7.2. Attività di controllo

Le attività di controllo assumono rilevanza sia in chiave preventiva, concorrendo ad evitare la realizzazione di atti fraudolenti, sia in chiave successiva consentendo di intercettare eventuali situazioni anomale (es. frodi perpetrate o indicatori di frode).

Tra le **misure di controllo preventive** assumono rilevanza, a titolo esemplificativo e non esaustivo:

- la definizione di ruoli e responsabilità coerente con il principio di segregazione delle attività;
- un sistema di poteri e livelli autorizzativi coerenti con il modello organizzativo definito;
- un sistema di autorizzazione e di monitoraggio degli accessi a beni e sistemi informativi aziendali;
- la tracciabilità dei processi le cui attività devono essere verificabili, documentate e ripercorribili nel tempo.

Tra le **misure di controllo successive** assumono rilevanza:

- le attività di *internal auditing*;
- le analisi di *data mining* atte a individuare possibili indicatori di anomalia sui quali focalizzare l'attenzione;
- il sistema di segnalazioni.

Alle misure di controllo di cui sopra, si aggiunge il **deterrente** (o *fraud deterrence*), ovvero il processo che consente di dissuadere la perpetrazione di atti fraudolenti attraverso:

- la definizione di un'esplicita e resa nota *fraud risk governance*;
- la creazione di una cultura antifrode;
- l'esecuzione di periodiche attività di *risk assessment*;
- l'implementazione di controlli antifrode;

- la presa di posizione nei confronti di atti fraudolenti identificati a seguito di attività investigative.

7.3. Attività di monitoraggio

Le attività di monitoraggio periodiche sono poste in essere dalla Funzione *Internal Audit* che, rispetto alle evidenze emerse, richiede a ciascuna delle Direzioni/Funzioni competenti di indicare le azioni correttive e i presidi di controllo implementati per far fronte ai *gap* identificati.

Apposita reportistica viene predisposta e sottoposta all'attenzione dei vertici aziendali e degli Organi di amministrazione e controllo del Gruppo SNAITECH.

8.1. Modalità di segnalazione

I Destinatari che abbiano evidenza – o abbiano il fondato sospetto – di violazioni della presente *policy* o di qualsiasi azione che possa delineare il rischio di frode potranno segnalare quanto accaduto alla Direzione Legale.

La Direzione Legale analizzerà la segnalazione ricevuta (anche relativamente alla sua veridicità e fondatezza) e provvederà alla gestione della stessa attivando, se necessario, le strutture/figure aziendali competenti per la definizione delle eventuali azioni correttive/misure disciplinari.

Qualora a seguito degli approfondimenti della segnalazione, la Direzione Legale valuti che la materia oggetto di segnalazione rientri nell'ambito di applicazione del Decreto *Whistleblowing*, procederà ad informare il Comitato *Whistleblowing* entro e non oltre 7 (sette) giorni dalla data di ricezione della segnalazione stessa. Il Comitato *Whistleblowing* - istituito presso ciascuna società del Gruppo SNAITECH - provvederà alla gestione della segnalazione secondo le modalità e prescrizioni definite nella *policy Whistleblowing* di riferimento (anche) per il tramite del Canale Informatico per le segnalazioni interne reso disponibile da ciascuna società, nel rispetto dei principi di confidenzialità e riservatezza.

Di tutto quanto sopra ne sarà informato prontamente il Segnalante nel totale rispetto della riservatezza della sua identità e del contenuto della segnalazione.

I Segnalanti possono inoltrare la segnalazione alla Direzione Legale tramite i canali di seguito indicati:

- E-mail all'indirizzo: segnalazionefrode@snaitech.it
- Posta ordinaria spedita all'indirizzo della sede legale della Società -Via Vittor Pisani, 22, Milano, 20124 – alla c.a. della Direzione Legale.

Al contempo, i destinatari della presente *policy* che ritengano di aver subito comportamenti ritorsivi (ad esempio, una minaccia di licenziamento, un demansionamento etc.) per essersi rifiutati di partecipare a fatti di cui hanno riconosciuto la matrice fraudolenta, devono inviare analoga segnalazione portando all'attenzione della medesima Direzione Legale quanto loro accaduto.

9. SVOLGIMENTO DELLE INDAGINI

L'avvio di investigazioni interne può derivare da numerosi eventi, tra cui, a titolo esemplificativo e non esaustivo:

- segnalazioni tramite il canale informatico *whistleblowing* o i canali alternativi;
- informazioni raccolte a seguito di attività di *internal auditing*;
- indicatori di anomalia sospetti;
- comunicazioni ufficiali o attività investigative da parte dell'Autorità giudiziaria.

Qualora, invece, l'investigazione accerti violazioni in capo a dipendenti, a componenti degli organi amministrativi o di controllo o a soggetti terzi, la Direzione Legale/il Comitato *Whistleblowing* interessa l'Organo Amministrativo della Società e le strutture/figure aziendali competenti per la definizione delle eventuali misure disciplinari e/o legali.

10. DOVERI DI FORMAZIONE

Il Gruppo SNAITECH e le società che ne fanno parte, ciascuna con riferimento al proprio ambito operativo, devono provvedere alla ricognizione e alla valutazione del rischio frode e, ove necessario, prevedere specifiche regole di comportamento per la realtà aziendale di riferimento attraverso l'adozione di appositi documenti normativi interni (procedure, *policy*, manuali operativi etc.). Ogni società è tenuta a prestare adeguata assistenza affinché i destinatari della presente *policy* siano messi in condizione di conformarsi a quanto in essa stabilito.

10.1 Erogazione della formazione al personale

Nell'ambito dei programmi di formazione al personale, devono essere previste sessioni di formazione in materia di prevenzione e contrasto di condotte di natura fraudolenta, da erogarsi o attraverso sessioni formative in presenza o, in alternativa, ricorrendo a tecnologie *e-learning*.

Il programma formativo deve riguardare:

- i rischi di frode cui sono esposti il Gruppo SNAITECH, le società che ne fanno parte e ciascuno dei Destinatari della presente *policy*;
- la politica di prevenzione adottata internamente al Gruppo;
- le azioni preventive da intraprendere e le segnalazioni da effettuare in relazione al rischio o al sospetto di verifica di fenomeni di natura fraudolenta.

È necessario conservare i programmi formativi ed i *report* delle presenze relativi alle predette sessioni di formazione.

10.2. La prevenzione dei fenomeni fraudolenti nell'ambito dei rapporti esterni

Terze parti, fornitori e consulenti devono essere informati dell'adozione della presente *policy* e deve essere loro richiesto, nell'intrattenere rapporti con il Gruppo SNAITECH e/o con ciascuna delle società ad esso appartenenti, di conformarsi scrupolosamente a quanto ivi stabilito.