MYGOLD SPA

Versione 01.1

Ultima revisione 01/02/2024

MANUALE DI CONFORMITÀ ANTIRICICLAGGIO

REDATTO MARCO PEDRAZZOLI
COMPLIANCE OFFICER

Sommario

GLOSSARIO

Adeguata Verifica (KYC-KYB): attività consistente nel:

- verificare l'identità del Cliente, dell'eventuale Esecutore e dell'eventuale Titolare effettivo sulla base di documenti, dati o informazioni ottenuti da una fonte affidabile e indipendente;
- acquisire informazioni sullo scopo e sulla natura prevista del rapporto continuativo e, quando rilevi secondo un approccio basato sul rischio, dell'operazione occasionale;
- esercitare un controllo costante nel corso del rapporto continuativo.

Alto dirigente: un amministratore o il direttore generale o altro dipendente delegato dall'organo con funzione di gestione o dal direttore generale a seguire i rapporti con la Clientela a rischio elevato; l'alto dirigente ha una conoscenza idonea del livello di Rischio di riciclaggio a cui è esposto il destinatario ed è dotato di un livello di autonomia sufficiente ad assumere decisioni in grado di incidere su questo livello di rischio.

Approccio basato sul rischio: indica un approccio in base al quale le autorità competenti e le imprese individuano, valutano e comprendono i Rischi di riciclaggio a cui le imprese sono esposte e adottano misure di contrasto commisurate a tali rischi.

Archivio Unico Informatico c.d. AUI: un archivio, formato e gestito a mezzo di sistemi informatici, nel quale sono conservate in modo accentrato tutte le informazioni acquisite nell'adempimento degli obblighi di adeguata verifica, secondo i principi previsti nel Decreto Antiriciclaggio e nei provvedimenti attuativi emanati dai Regulator.

Attività istituzionale: l'attività per la quale i destinatari hanno ottenuto l'iscrizione ovvero l'autorizzazione da parte di un'Autorità Pubblica.

Banca di Comodo: la banca (o l'intermediario finanziario che svolge funzioni analoghe ad una banca) priva di una struttura significativa nel paese in cui è stata costituita e autorizzata all'esercizio dell'attività e non appartenente ad un gruppo finanziario soggetto a un'efficace vigilanza su base consolidata.

Beneficiario della prestazione assicurativa:

1. la persona fisica o l'entità diversa da una persona fisica che, sulla base della designazione effettuata dal contraente o dall'assicurato, ha diritto di percepire la prestazione assicurativa corrisposta dall'impresa di assicurazione;
2. l'eventuale persona fisica o entità diversa da una persona fisica a favore della quale viene effettuato il pagamento su disposizione del beneficiario designato.

Cliente/Clientela: il soggetto che instaura rapporti continuativi o compie operazioni con Banchi Metalli, intermediari finanziari e altri soggetti esercenti attività finanziaria nonché con altri destinatari degli obblighi di cui al Decreto Antiriciclaggio, normalmente individuati anche con altri termini, quali utenti, investitori, assicurati, contraenti, acquirenti, affidati, ecc.

Compliance Risk: specifico adempimento richiesto da una determinata normativa, per non incorrere in sanzioni giudiziarie o amministrative, perdite finanziarie rilevanti o danni di reputazione in conseguenza di violazioni di norme imperative (leggi, regolamenti) o di autoregolamentazione (ad esempio codice di condotta, codice di autodisciplina).

Congelamento di fondi: il divieto, in virtù dei regolamenti comunitari e della normativa nazionale, di movimentazione, trasferimento, modifica, utilizzo o gestione dei fondi in genere o di accesso ad essi, così da modificarne il volume, l'importo, la collocazione, la proprietà, il possesso, la natura, la destinazione o qualsiasi altro cambiamento che consente l'uso dei fondi, compresa la gestione di portafoglio.

Congelamento di risorse economiche: il divieto, in virtù dei regolamenti comunitari e della normativa nazionale, di trasferimento, disposizione o, al fine di ottenere in qualsiasi modo fondi, beni o servizi, utilizzo delle risorse economiche, compresi, a titolo meramente esemplificativo, la vendita, la locazione, l'affitto o la costituzione di diritti reali di garanzia.

Conti correnti di corrispondenza e rapporti ad essi assimilabili: conti tenuti dalle banche per il regolamento dei servizi interbancari e altri rapporti comunque denominati, intrattenuti tra enti creditizi e istituti finanziari, utilizzati per il regolamento di transazioni per conto dei Clienti degli enti corrispondenti.

Conti di passaggio: rapporti bancari di corrispondenza transfrontalieri, intrattenuti tra intermediari bancari e finanziari ed Exchange, utilizzati per effettuare operazioni in nome proprio e per conto della Clientela.

Controlli di linea (c.d. "controlli di primo livello"): l'insieme dei controlli diretti ad assicurare il corretto svolgimento delle operazioni. Essi sono effettuati dalle stesse Strutture Operative (ad es. controlli di tipo gerarchico, sistematici e a campione), anche attraverso unità dedicate esclusivamente a compiti di controllo o presidio che riportano ai responsabili delle Strutture Operative, ovvero eseguiti nell'ambito del back office; per quanto possibile, essi sono incorporati nelle procedure informatiche.

Controlli sui rischi e sulla conformità (c.d. "controlli di secondo livello"): l'insieme dei controlli che hanno l'obiettivo di assicurare, tra l'altro:

- la corretta attuazione del processo di gestione dei rischi;
- il rispetto dei limiti operativi assegnati alle varie funzioni;
- la conformità dell'operatività aziendale alle norme, incluse quelle di autoregolamentazione.

Le funzioni preposte a tali controlli sono distinte da quelle operative; esse concorrono alla definizione delle politiche di governo dei rischi e del processo di gestione dei rischi.

Controparte: persone fisiche e giuridiche che instaurano una relazione d'affari con il Banco Metalli MyGOLD (anche se non destinatarie degli obblighi di cui al Decreto Antiriciclaggio).

Cover Payment (o pagamento di copertura): il trasferimento di fondi utilizzato quando non vi è un rapporto diretto tra prestatore di servizi di pagamento (c.d. PSP) dell'ordinante e del Beneficiario ed è quindi necessario ricorrere ad una catena di rapporti di corrispondenza tra PSP. In un pagamento di copertura sono coinvolti tre o più PSP.

Criptovaluta: Una criptovaluta è una valuta virtuale che, secondo la definizione di Banca d'Italia, costituisce una rappresentazione digitale di valore ed è utilizzata come mezzo di scambio o detenuta a scopo di investimento. Le criptovalute possono essere trasferite, conservate o negoziate elettronicamente. Alcuni esempi tipici sono il Bitcoin, LiteCoin, Ripple, Ethereum, Cardano, Tron.

Dati identificativi del Cliente, del relativo Titolare effettivo e dell'Esecutore: il nome e il cognome, il luogo e la data di nascita, la residenza anagrafica e, ove diverso, il domicilio, e, ove assegnato, il codice

fiscale del Cliente, e ove ne sia prevista l'assegnazione, anche il relativo Titolare effettivo e dell'Esecutore. Nel caso di soggetti diversi da persona fisica, la denominazione, la sede legale, il numero di iscrizione nel registro delle imprese ovvero nel registro delle persone giuridiche ove previsto. In entrambi i casi, al momento della liquidazione della prestazione, anche la residenza anagrafica e, ove diverso, il domicilio, il codice fiscale del Beneficiario e, ove ne sia prevista l'assegnazione, anche del relativo Titolare effettivo e dell'Esecutore.

Dati identificativi del Beneficiario, del relativo Titolare effettivo e dell'Esecutore: il nome e il cognome, luogo e data di nascita. Nel caso di soggetti diversi da persona fisica, la denominazione, la sede legale, il numero di iscrizione nel registro delle imprese ovvero nel registro delle persone giuridiche ove previsto. In entrambi i casi, al momento della liquidazione della prestazione, anche la residenza anagrafica e, ove diverso, il domicilio, il codice fiscale del Beneficiario e, ove ne sia prevista l'assegnazione, anche del relativo Titolare effettivo e dell'Esecutore.

Denaro contante: le banconote e le monete metalliche, in euro o in valute estere, aventi corso legale. (**MyGOLD SpA come Banco Metalli non accetta pagamenti in cash – denaro effettivo**)

Dipendente: tutti i dipendenti di MyGOLD SpA, siano essi appartenenti alle unità organizzative e/o alle strutture territoriali e/o alle strutture centrali.

Esecutore: il soggetto delegato ad operare in nome e per conto del Cliente o a cui siano comunque conferiti poteri di rappresentanza che gli consentano di operare in nome e per conto del Cliente.

Fattori di rischio: indicano le variabili suscettibili, singolarmente o in combinazione tra loro, di accrescere o ridurre il Rischio di riciclaggio derivante da singoli rapporti continuativi o operazioni occasionali.

Financial Advisor: i consulenti finanziari di MyGOLD SpA abilitati all'offerta fuori sede. Svolgono l'attività di consulenza indipendente e forniscono consulenza in materia di acquisto, vendita, deposito dei metalli preziosi. Il Financial Advisor opera in modo indipendente nei confronti dei propri clienti.

Fondi: le attività ed utilità finanziarie di qualsiasi natura, possedute anche per interposta persona fisica o giuridica, compresi a titolo meramente esemplificativo:

- i contanti, gli assegni, i crediti pecuniari, le cambiali, gli ordini di pagamento e altri strumenti di pagamento;
- i depositi presso enti finanziari o altri soggetti, i saldi sui conti, i crediti e le obbligazioni di qualsiasi natura;
- i titoli negoziabili a livello pubblico e privato nonché gli strumenti finanziari;
- gli interessi, i dividendi o altri redditi ed incrementi di valore generati dalle attività;
- il credito, il diritto di compensazione, le garanzie di qualsiasi tipo, le cauzioni e gli altri impegni finanziari;
- le lettere di credito, le polizze di carico e gli altri titoli rappresentativi di merci;
- tutti gli altri strumenti di finanziamento delle esportazioni;
- le polizze assicurative concernenti i rami vita di cui all'articolo;
- Crypto Currency (Bitcoin, Ethereum, ecc.);
- Stable Coin (Tether, USC, ecc.);
- Equity token;
- Utility Token;
- NFT – Non-fungible Token;
- Security Token.

Funzione Antiriciclaggio: la funzione, parte integrante del sistema dei controlli interni di secondo livello, deputata a prevenire e contrastare i fenomeni nonché la realizzazione di operazioni di riciclaggio e di finanziamento del terrorismo.

Funzioni Aziendali di Controllo: la Funzione Compliance, la Funzione Risk Management, la Funzione Antiriciclaggio, la Funzione Internal Audit.

Funzione Compliance: la Funzione a cui è affidato il compito specifico di presiedere, secondo un approccio risk-based, alla gestione del rischio di non conformità con riguardo all'attività aziendale, verificando che le procedure siano adeguate a prevenire tale rischio, consistente nella violazione di norme di etero regolamentazione (leggi e regolamenti) e autoregolamentazione (codici di condotta, codici etici) applicabili al Banco Metalli MyGOLD. Detta Funzione è parte integrante del sistema dei controlli interni.

Funzioni di Controllo: le Funzioni Aziendali di Controllo, il Dirigente Preposto, l'Amministratore Incaricato dei Controlli, il personale addetto alla gestione dell'identificazione dei clienti.

Funzione Internal Audit: la Funzione cui è affidato il compito di presidiare, in ottica di controlli di terzo livello, anche con verifiche in loco, il regolare andamento dell'operatività e l'evoluzione dei rischi e a valutare la completezza, l'adeguatezza, la funzionalità e l'affidabilità della struttura organizzativa e delle altre componenti del Sistema dei Controlli Interni, portando all'attenzione degli organi aziendali i possibili miglioramenti, con particolare riferimento al **Risk Appetite Framework (RAF)**, al processo di gestione dei rischi nonché agli strumenti di misurazione e controllo degli stessi. Sulla base dei risultati dei propri controlli, formula raccomandazioni agli organi aziendali.

Indicatori di anomalia: fattispecie rappresentative di operatività ovvero di comportamenti anomali posti in essere dalla clientela, finalizzate ad agevolare la valutazione, da parte dei soggetti obbligati, degli eventuali profili di sospetto di riciclaggio o di finanziamento del terrorismo.

Mezzi di pagamento: il denaro contante **(non accettato nelle transazioni da MyGOLD SpA)**, gli assegni bancari e postali, gli assegni circolari e gli altri assegni a essi assimilabili o equiparabili, i vaglia postali, gli ordini di accreditamento o di pagamento, le carte di credito e le altre carte di pagamento, le polizze assicurative trasferibili, le polizze di pegno e ogni altro strumento a disposizione che permetta di trasferire, movimentare o acquisire, anche per via telematica, fondi, valori o disponibilità finanziarie.

Operatività a distanza: l'operatività svolta senza la presenza fisica del cliente e del personale incaricato del Banco Metalli. Quando il cliente è un soggetto diverso da una persona fisica, si considera presente quando lo è l'esecutore.

Operazione: l'attività consistente nella movimentazione, nel trasferimento o nella trasmissione di ordini di acquisto, vendita di metalli preziosi; costituisce operazione anche la stipulazione di un atto negoziale, a contenuto patrimoniale, rientrante nell'esercizio dell'attività professionale o commerciale.

Operazioni collegate: le operazioni tra loro connesse per il perseguimento di un unico obiettivo di carattere giuridico patrimoniale.

Operazione frazionata: un'operazione unitaria sotto il profilo del valore economico, di importo pari o superiore ai limiti stabiliti dal Decreto Antiriciclaggio, posta in essere attraverso più operazioni, singolarmente inferiori ai predetti limiti, effettuate in momenti diversi ed in un circoscritto periodo di

tempo fissato in sette giorni, ferma restando la sussistenza dell'operazione frazionata quando ricorrano elementi per ritenerla tale.

Operazione occasionale: un'operazione non riconducibile a un rapporto continuativo in essere; costituisce operazione occasionale anche la prestazione intellettuale o commerciale, ivi comprese quelle ad esecuzione istantanea, resa in favore del Cliente.

Operazione Sospetta: l'operazione che per caratteristiche, entità, natura, nonché per collegamento con altre operazioni o per frazionamento della stessa o per qualsivoglia altra circostanza conosciuta in ragione delle funzioni esercitate, tenuto conto anche della capacità economica e dell'attività svolta dal soggetto cui è riferita, in base agli elementi acquisiti ai sensi del Decreto Antiriciclaggio, induce a ritenere, sospettare, o ad avere ragionevoli motivi per sospettare che siano in corso o che siano state compiute o tentate operazioni di riciclaggio o finanziamento del terrorismo o che comunque, indipendentemente dalla loro entità, provengano da attività criminosa.

Organi aziendali: il complesso degli Organi con funzioni di supervisione strategica (Consiglio di Amministrazione), di gestione (Amministratore Delegato o altro Organo cui è assegnata la funzione di gestione) e di controllo (Collegio Sindacale).

Organo con funzione di controllo: Organo che verifica la regolarità dell'attività di amministrazione e l'adeguatezza degli assetti organizzativi e contabili della Società; il Collegio Sindacale, il Consiglio di sorveglianza e il comitato per il controllo sulla gestione sono, nei diversi modelli, gli Organi con funzione di controllo (o Organi di controllo).

Organo con funzione di gestione: Organo aziendale o componenti di esso ai quali spettano o sono delegati compiti di gestione, ossia l'attuazione degli indirizzi deliberati nell'esercizio della funzione di supervisione strategica. Il direttore generale rappresenta il vertice della struttura interna e come tale partecipa alla funzione di gestione.

Organismo con funzione di supervisione strategica: organismo responsabile di tutti gli orientamenti e/o la supervisione della gestione aziendale (ad esempio, attraverso l'esame e l'approvazione dei piani aziendali o finanziari o delle operazioni strategiche realizzate dalla Società).

Origine dei fondi: indica la provenienza dei fondi specificatamente impiegati in un rapporto continuativo o in una operazione occasionale.

Origine del patrimonio: indica l'origine del patrimonio complessivo del Cliente, ricomprendendo sia le attività mobiliari che quelle immobiliari. Il Banco Metalli MyGOLD cosciente che opera in un mercato particolare, ha integrato nei propri sistemi di controllo parametri definiti per attivare controlli supplementari in presenza di scambi o depositi che richiedano informazioni aggiuntive sulla provenienza. In MyGOLD SpA, chi attiva il proprio Account, deve in ogni caso superare tutte le procedure KYC-KYB e AML per poter iniziare ad operare.

Paesi comunitari: Paesi appartenenti allo Spazio economico europeo.

Paesi terzi: Paesi non appartenenti allo Spazio economico europeo.

Paesi terzi ad alto rischio: paesi non appartenenti all'Unione Europea i cui ordinamenti presentano carenze strategiche nei rispettivi regimi nazionali di prevenzione del riciclaggio e del finanziamento del terrorismo.

Personale: i dipendenti e coloro che comunque operano sulla base di rapporti che ne determinano l'inserimento nell'organizzazione del soggetto obbligato, anche in forma diversa dal rapporto di lavoro subordinato, ivi compresi i Financial Advisor abilitati alla consulenza indipendente.

Persone Esposte Politicamente (PEP): le persone fisiche, ovverosia "le persone fisiche che occupano o hanno cessato di occupare da meno di un anno importanti cariche pubbliche, nonché i loro familiari e coloro che con i predetti soggetti intrattengono notoriamente stretti legami, come di seguito elencate:

1. sono persone fisiche che occupano o hanno occupato importanti cariche pubbliche coloro che ricoprono o hanno ricoperto la carica di:

    1.1. Presidente della Repubblica, Presidente del Consiglio, Ministro, Vice-Ministro e Sottosegretario, Presidente di Regione, assessore regionale, Sindaco di capoluogo di provincia o città metropolitana, Sindaco di comune con popolazione non inferiore a 15.000 abitanti nonché cariche analoghe in Stati esteri;
    1.2. deputato, senatore, parlamentare europeo, consigliere regionale nonché cariche analoghe in Stati esteri;
    1.3. membro degli organi direttivi centrali di partiti politici;
    1.4. giudice della Corte Costituzionale, magistrato della Corte di Cassazione o della Corte dei conti, consigliere di Stato e altri componenti del Consiglio di Giustizia Amministrativa per la Regione siciliana nonché cariche analoghe in Stati esteri;
    1.5. membro degli organi direttivi delle banche centrali e delle autorità indipendenti;
    1.6. ambasciatore, incaricato d'affari ovvero cariche equivalenti in Stati esteri, ufficiale di grado apicale delle forze armate ovvero cariche analoghe in Stati esteri;
    1.7. componente degli organi di amministrazione, direzione o controllo delle imprese controllate, anche indirettamente, dallo Stato italiano o da uno Stato estero ovvero partecipate, in misura prevalente o totalitaria, dalle Regioni, da comuni capoluoghi di provincia e città metropolitane e da comuni con popolazione complessivamente non inferiore a 15.000 abitanti;
    1.8. direttore generale di ASL e di azienda ospedaliera, di azienda ospedaliera universitaria e degli altri enti del servizio sanitario nazionale;
    1.9. direttore, vicedirettore e membro dell'organo di gestione o soggetto svolgenti funzioni equivalenti in organizzazioni internazionali.

2. sono familiari di persone politicamente esposte: i genitori, il coniuge o la persona legata in unione civile o convivenza di fatto o istituti assimilabili alla persona politicamente esposta, i figli e i loro coniugi nonché le persone legate ai figli in unione civile o convivenza di fatto o istituti assimilabili;

3. sono soggetti con i quali le persone politicamente esposte intrattengono notoriamente stretti legami:

    3.1. le persone fisiche legate alla persona politicamente esposta per via della titolarità effettiva congiunta di enti giuridici (inclusi trust e istituti giuridici affini) ovvero che intrattengono con la persona politicamente esposta stretti rapporti d'affari;
    3.2. le persone fisiche che detengono solo formalmente il controllo totalitario di un'entità notoriamente costituita, di fatto, nell'interesse e a beneficio di una persona politicamente esposta.

Piattaforma centralizzata: è la piattaforma che si riconduce ad un proprietario che ne determina

norme e funzioni in modo autonomo. Possiamo definire piattaforme centralizzate le Banche, le Assicurazioni ecc. Nel caso di MyGOLD SpA al fine di rispettare le norme AML e KYC e KYB, ha deciso di operare in modo centralizzato, volendo identificare ogni operazione eseguita al suo interno.

Policy antiriciclaggio o Policy: il documento definito dall'organo con funzione di gestione e approvato dall'organo con funzione di supervisione strategica ai sensi delle Disposizioni in materia di organizzazione, procedure e controlli interni volti a prevenire l'utilizzo degli intermediari a fini di riciclaggio e di finanziamento del terrorismo.

PSP: Prestatore di Servizi di Pagamento.

Prestatori di servizi di informazione sui conti (AISP): è un Prestatore di Servizi di Pagamento che fornisce servizi di informazione sui conti, ovvero servizi online che forniscono informazioni consolidate relativamente a uno o più conti di pagamento detenuti dall'utente di servizi di pagamento presso un altro Prestatore di servizi di pagamento o presso più prestatori di servizi di pagamento.

Prestatori di servizi di portafoglio digitale: ogni persona fisica o giuridica che fornisce a terzi, a titolo professionale, anche online, servizi di salvaguardia di chiavi crittografiche private per conto dei propri Clienti, al fine di detenere, memorizzare e trasferire valute virtuali.

Prestatori di servizi relativi all'utilizzo di valuta virtuale: ogni persona fisica o giuridica che fornisce a terzi, a titolo professionale, servizi funzionali all'utilizzo, allo scambio, alla conservazione di valuta virtuale e alla loro conversione da ovvero in valute aventi corso legale.

Rapporto continuativo: un rapporto di durata, rientrante nell'esercizio dell'attività di istituto svolta dai soggetti obbligati, che non si esaurisce in un'unica operazione.

Rapporti o operazioni a distanza: indica qualsiasi operazione o rapporto in cui il cliente non è fisicamente presente, ossia non si trova nello stesso luogo fisico dell'impresa o di una persona che agisce per conto di detta impresa. Ciò comprende le situazioni in cui l'identità del cliente viene verificata tramite collegamento video o mezzi tecnologici simili.

Risk appetite: il livello di rischio (complessivo e per tipologia) che la Società intende assumere per il perseguimento dei suoi obiettivi strategici.

Rischio di riciclaggio: il rischio derivante dalla violazione di previsioni di legge, regolamentari e di autoregolamentazione funzionali alla prevenzione dell'uso del sistema finanziario per finalità di riciclaggio, di finanziamento del terrorismo o di finanziamento dei programmi di sviluppo delle armi di distruzione di massa, nonché il rischio di coinvolgimento in episodi di riciclaggio e di finanziamento del terrorismo o di finanziamento dei programmi di sviluppo delle armi di distruzione di massa.

Rischio inerente: nella logica del c.d. rischio "potenziale", la probabilità per la Società di subire un danno diretto od indiretto di natura sanzionatoria, penale, finanziaria o reputazionale senza considerare l'organizzazione ed il funzionamento dei propri presidi organizzativi ed il più generale Sistema dei Controlli Interni.

Rischio residuo: giudizio di sintesi che tiene conto della valutazione dell'idoneità dei presidi organizzativi, procedurali e di controllo in essere, con conseguente individuazione delle iniziative correttive da intraprendere ai fini della sua mitigazione.

Risorse economiche: le attività di qualsiasi tipo, materiali o immateriali e i beni, mobili o immobili, ivi

compresi gli accessori, le pertinenze e i frutti, che non sono fondi ma che possono essere utilizzate per ottenere fondi, beni o servizi, possedute, detenute o controllate, anche parzialmente, direttamente o indirettamente, ovvero per interposta persona fisica o giuridica, da parte di soggetti designati, ovvero da parte di persone fisiche o giuridiche che agiscono per conto o sotto la direzione di questi ultimi.

Sistema dei controlli interni: l'insieme delle regole, delle funzioni, delle strutture, delle risorse dei processi e delle procedure che mirano ad assicurare, nel rispetto della sana e prudente gestione, le seguenti finalità:

- verifica dell'attuazione delle strategie e delle politiche aziendali;
- contenimento del rischio entro i limiti indicati nel quadro di riferimento per la determinazione della propensione al rischio del Banco Metalli MyGOLD SpA (**Risk Appetite Framework - "RAF**");
- salvaguardia del valore delle attività e protezione dalle perdite;
- efficacia ed efficienza dei processi aziendali;
- affidabilità e sicurezza delle informazioni aziendali e delle procedure informatiche;
- prevenzione del rischio che il Banco Metalli sia coinvolto, anche involontariamente, in attività illecite (con particolare riferimento a quelle connesse con il riciclaggio, l'usura ed il finanziamento al terrorismo);
- conformità delle operazioni con la legge e la normativa di vigilanza, nonché con le politiche, i regolamenti e le procedure interne.

Titolare effettivo: la persona fisica o le persone fisiche, diverse dal Cliente, nell'interesse della quale o delle quali, in ultima istanza, il rapporto continuativo è istaurato, la prestazione professionale è resa o l'operazione è eseguita.

Token: i token sono paragonati alle criptovalute, pur mantenendo a seconda dei casi funzione e attributi differenti, che non rientrano nella sola mera attività di scambio, ma possono apportare diritti specifici ai possessori che le detengono. Vengono in ogni caso gestiti in modo digitale mediante un wallet dedicato.

Valuta virtuale: la rappresentazione digitale di valore, non emessa da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi e trasferita, archiviata e negoziata elettronicamente.

Account: il conto deposito detenuto da un cliente del Banco Metalli MyGOLD SpA, in grado di custodire metalli preziosi con il fine di consentire la normale operatività di acquisto, vendita, deposito.

0.0 PREMESSE

Il riciclaggio e il finanziamento del terrorismo rappresentano fenomeni criminali che, anche in virtù della loro possibile dimensione transnazionale, costituiscono una grave minaccia per l'economia legale e possono determinare effetti destabilizzanti, soprattutto per il sistema bancario e finanziario. La natura mutevole delle minacce del riciclaggio e del finanziamento del terrorismo, facilitata anche dalla continua evoluzione della tecnologia e dei mezzi a disposizione dei criminali, richiede un costante adattamento dei presidi di prevenzione e contrasto. Le raccomandazioni necessarie applicate in questo segmento di mercato prevedono che le autorità pubbliche e il settore privato identifichino e valutino i Rischi di riciclaggio cui sono esposti, al fine di adottare adeguate misure di mitigazione. L'azione di prevenzione e contrasto del riciclaggio si esplica attraverso l'introduzione di presidi volti a garantire la piena conoscenza del Cliente, la tracciabilità delle transazioni finanziarie e l'individuazione delle operazioni sospette. L'intensità dei presidi di prevenzione e contrasto deve essere modulata secondo un approccio basato sul rischio (c.d. **Risk-Based Approach**), focalizzato sulle ipotesi meritevoli di maggiore scrutinio e realizzato rendendo più efficace l'attività di monitoraggio e più efficiente l'allocazione delle risorse. Tale approccio costituisce il punto cardine per il comportamento dei soggetti obbligati e per l'azione di controllo della Autorità. MyGold S.P.A. (in seguito anche "Società" o "Banco Metalli") è fortemente impegnata nell'evitare che i prodotti e i servizi offerti siano utilizzati per finalità criminali di riciclaggio e di finanziamento del terrorismo, promuovendo al loro interno una cultura improntata al pieno rispetto delle disposizioni vigenti e all'efficace assolvimento degli obblighi di collaborazione passiva, finalizzata a garantire la conoscenza approfondita della Clientela e la conservazione dei documenti relativi alle transazioni effettuate, e di collaborazione attiva, volta all'individuazione e segnalazione delle operazioni sospette di riciclaggio. In particolare, spetta al Consiglio di Amministrazione individuare politiche di governo di detti rischi adeguate all'entità e alla tipologia dei profili di rischio cui è concretamente esposta l'attività del Banco Metalli MyGold S.P.A., tenendo conto degli esiti dell'esercizio di autovalutazione dei rischi di riciclaggio e finanziamento del terrorismo, il quale costituisce il presupposto per la definizione e la manutenzione dei presidi di tali rischi. L'Amministratore Delegato appronta le procedure necessarie per dare attuazione a tali politiche; la Funzione Antiriciclaggio ne verifica, nel continuo, l'idoneità al fine di assicurare un adeguato presidio dei citati rischi, coordinandosi con le altre funzioni aziendali di controllo. L'Internal Audit verifica in modo continuativo il grado di adeguatezza dell'assetto organizzativo aziendale e la sua conformità rispetto alla disciplina di riferimento e vigila sulla funzionalità del complessivo sistema dei controlli interni. Un'efficace attività di prevenzione dei rischi non può, in ogni caso, essere demandata alle sole funzioni di controllo, ma deve svolgersi, in primo luogo, dove il rischio viene generato, in particolare nell'ambito delle linee operative. Le Strutture Operative sono, quindi, le prime responsabili del processo di gestione dei rischi: nel corso dell'operatività giornaliera tali strutture devono identificare, misurare o valutare, monitorare, attenuare e riportare i rischi derivanti dall'ordinaria attività aziendale, in conformità con il processo di gestione dei rischi. In tale ambito, assumono particolare rilevanza i "consulenti finanziari della Rete di Consulenza" e i "dipendenti delle unità organizzative" cui compete l'amministrazione e la gestione concreta dei rapporti con la clientela: a tali soggetti, infatti, è attribuita la responsabilità di monitorarne l'operatività e segnalare eventuali operazioni sospette, nel rispetto delle apposite linee guida predisposte dal Banco Metalli. Nell'ottica di assicurare un'efficace prevenzione dei rischi di non conformità alla normativa, è inoltre fondamentale che le diverse strutture aziendali assicurino, in caso di offerta di prodotti e servizi nuovi, il tempestivo coinvolgimento della Funzione Antiriciclaggio, affinché quest'ultima possa effettuare in via preventiva le proprie valutazioni.

SEZIONE 1. INTRODUZIONE E DICHIARAZIONI POLITICHE

1.1 POLITICA

MYGOLD SPA, è una società costituita come S.P.A. (Società per Azioni) in Italia, Milano, (la "Società"), registrare la propria attività presso Banca D'Italia con licenza n. 5008800 impegnandosi a far rispettare le leggi per prevenire il riciclaggio di denaro, il finanziamento del terrorismo, la proliferazione e il finanziamento della proliferazione e altre transazioni illegali. È politica della Società garantire che standard etici elevati siano mantenuti e agire in modo conforme a tutte le leggi, i regolamenti, le regole e le dichiarazioni normative di linee guida e principi rilevanti per la propria attività.

Il manuale è applicabile a tutto il personale della Società, inclusi tutti i funzionari, direttori, dirigenti, amministratori e personale ausiliario e non è limitato alle persone che lavorano con contratto di lavoro, ma comprende anche il personale a tempo determinato e a contratto.

1.2 SCOPO

Lo scopo di questo Manuale di conformità antiriciclaggio è rispettare la legislazione e i regolamenti del AML previsto secondo i dettami della Banca D'Italia e la Banca Centrale Europea, e delle norme disposte dall'ESMA (European Securities and Markets Autority), fornendo al tempo stesso al personale le risorse per consentire loro di adempiere ai propri obblighi personali e aziendali ai sensi del quadro legislativo dello stato italiano, includendo per estensione la comunità europea, per la prevenzione del riciclaggio di denaro, finanziamento del terrorismo, proliferazione e finanziamento della proliferazione delle attività descritte in maggiore dettaglio nella sezione intitolata "Quadro legislativo" del presente manuale.

Tutto il personale interessato deve essere a conoscenza dell'esistenza e del contenuto di questo manuale, portando immediatamente qualsiasi anomalia o preoccupazione all'attenzione del Funzionario di conformità antiriciclaggio ("**AMLCO – Anti-Money Laundering Compliance Officer**)") e/o degli Amministratori, a seconda dei casi.

Questa guida non intende essere un'alternativa alla lettura delle disposizioni pertinenti della Legge su atti criminali previsti dall'ordinamento dello Stato di Italiano e della Comunità Europea mediante gli organi di vigilanza e le Autority preposte. Tutto il personale è tenuto a firmare una conferma di aver letto e compreso le politiche e le procedure e di essere consapevole dei propri obblighi personali. Tale conferma sarà conservata dall'AMLCO e aggiornata ogni volta che il manuale cambia.

Gli Amministratori hanno approvato il presente manuale e dovranno approvare eventuali successive modifiche.

1.3 RESPONSABILITÀ DELLA POLITICA ANTIRICICLAGGIO

Sebbene gli Amministratori mantengano la responsabilità generale di tutte le politiche e procedure, compreso il presente manuale, gli Amministratori possono delegare la responsabilità per la produzione e l'aggiornamento del presente manuale a un funzionario della Società che dovrebbe agire in consultazione con l'AMLCO. Incluso, la società può avvalersi di società e consulenti esterni per la gestione delle fasi relative alle procedure AML.

Inoltre, se il personale viene a conoscenza di anomalie in questo manuale che potrebbero essere contraddittorie con le attuali procedure pratiche, l'alta dirigenza, **MLRO- Money Laundering**

Reporting Officer, **DMLRO- Deputy Money Laundering Reporting Officer** e/o **AMLCO- Anti-Money Laundering Compliance Officer** devono essere immediatamente informati. La Società ha nominato responsabili del Programma Antiriciclaggio i seguenti soggetti:

Director Compliance Officer	Nome: Marco Pedrazzoli
Money Laundering Reporting Officer ("MLRO")	Nome: Ernesto Vargas
Deputy Money Laundering Reporting Officer ("DMLRO")	Nome: Paola Beccerica
Anti-Money Laundering Compliance Officer ("AMLCO")	Nome: Luca Canella

1.4 RESPONSABILITÀ DEL PERSONALE

La Società richiede a tutto il personale di essere a conoscenza dei propri obblighi personali in materia di antiriciclaggio previsti dalla normativa e dai regolamenti. Tutto il personale è tenuto a leggere e seguire le procedure contenute nel presente manuale, in quanto il mancato mantenimento di un'adeguata consapevolezza e il mancato rispetto di procedure commisurate alla posizione di un individuo all'interno dell'Azienda può comportare provvedimenti disciplinari interni, diminuzione dei compensi e/o cessazione del rapporto di lavoro.

Inoltre, nel caso in cui venga rilevata un'attività sospetta o insolita, i successivi procedimenti giudiziari possono comportare la sospensione e, in ultima analisi, un'azione penale se un individuo viene ritenuto negligente nell'adempiere ai propri obblighi. Indipendentemente dall'esito di eventuali procedimenti giudiziari, il consiglio di amministrazione con la guida dell'AMLCO in collaborazione con l'MLRO può determinare se un individuo ha adeguatamente adempiuto ai propri obblighi e mantenuto un'adeguata consapevolezza commisurata alle aspettative. Il mancato rispetto di tali obblighi può costituire motivo di licenziamento dalla Società.

Tutti i committenti e il personale, indipendentemente dal loro livello di anzianità, riceveranno aggiornamenti regolari e una formazione annuale sulle tendenze attuali in materia di riciclaggio di denaro, finanziamento del terrorismo e proliferazione, al fine di aiutarli a rimanere vigili in modo da essere in grado di rilevare questioni che sembrano essere di natura insolita, in particolare quelle che potrebbero essere indicative di attività illegali.

Eventuali preoccupazioni relative alla capacità di un individuo di adempiere agli obblighi personali o aziendali devono essere portate immediatamente all'attenzione dell'alta dirigenza e/o dell'AMLCO-Anti-Money Laundering Compliance Officer.

SEZIONE 2. RICICLAGGIO DI DENARO E FINANZIAMENTO DEL TERRORISMO

2.1 COS'È IL RICICLAGGIO DI DENARO?

Il riciclaggio di denaro è il processo mediante il quale i criminali cercano di mascherare l'identità e la vera fonte del loro reddito illegale e farlo sembrare legittimo. I criminali riciclano denaro per evitare di essere scoperti dalle forze dell'ordine e fare uso personale di proventi illeciti, comprese ulteriori attività criminali e investimenti in attività legittime.

2.2 COS'È IL FINANZIAMENTO DEL TERRORISMO?

Il finanziamento al terrorismo può essere definito come la fornitura di fondi a un'organizzazione con l'intenzione che dovrebbero essere utilizzati, o la consapevolezza che devono essere utilizzati, per commettere un atto terroristico. Gli esperti generalmente ritengono che il finanziamento del terrorismo provenga da due fonti primarie. La prima fonte è il sostegno finanziario fornito da stati o organizzazioni con infrastrutture sufficientemente grandi per raccogliere e quindi mettere fondi a disposizione delle cellule terroristiche. La seconda principale fonte di fondi per le organizzazioni terroristiche è il reddito derivato direttamente da varie attività "generatrici di entrate".

Sebbene questo manuale parli di riciclaggio di denaro in termini generali, è importante che il personale sia consapevole del fatto che il finanziamento al terrorismo può presentarsi in modo simile a quello del riciclaggio di denaro o con altri mezzi a sé stanti. I fondi utilizzati per sostenere il terrorismo possono provenire da fonti legittime, attività criminali o entrambe.

2.3 COS'È LA PROLIFERAZIONE E IL FINANZIAMENTO DELLA PROLIFERAZIONE?

La proliferazione è la fabbricazione, l'acquisizione, il possesso, lo sviluppo, l'esportazione, il trasbordo, l'intermediazione, il trasporto, il trasferimento, lo stoccaggio o l'uso di armi nucleari, chimiche o biologiche e dei loro mezzi di consegna e dei relativi materiali (compresi sia le tecnologie che i beni a duplice uso utilizzati per scopi non legittimi), in violazione delle leggi nazionali o, ove applicabili, degli obblighi internazionali. Include tecnologia, beni, software, servizi e competenze.

Il finanziamento della proliferazione è l'atto di fornire fondi o servizi finanziari che vengono utilizzati, in tutto o in parte, per rendere possibile la proliferazione. In altre parole, è il finanziamento delle attività di proliferazione.

Sebbene questo manuale parli di riciclaggio di denaro in termini generali, è importante che il personale sia consapevole del fatto che la proliferazione e il finanziamento della proliferazione possono presentarsi in modo simile a quello del riciclaggio di denaro o con altri mezzi a sé stanti. A differenza del riciclaggio di denaro, che riguarda i fondi raccolti con mezzi illegittimi, la fonte dei fondi utilizzati per finanziare la proliferazione può essere sia legale che illegale. La destinazione o l'uso di tali fondi serve a far avanzare le ambizioni degli stati sanzionatori. In molti casi, la fonte di finanziamento proviene da uno stato o da una persona che agisce come agente indiretto dello stato. Pertanto, mentre alcuni indicatori di rischio ed elementi di controllo potrebbero sovrapporsi per il riciclaggio di denaro e il finanziamento della proliferazione, il finanziamento della proliferazione ha anche i suoi indicatori di rischio unici.

2.4 RISCHI E VULNERABILITÀ AML/CFT CON L'ACQUISTO DI METALLI PREZIOSI MEDIANTE L'USO DI MONETA DIGITALE E MONETA FIAT

I metalli preziosi che possono essere scambiati, acquistati e venduti con denaro reale (FIAT) o anche attraverso l'utilizzo di valute virtuali, sono potenzialmente vulnerabili al riciclaggio di denaro e all'abuso di finanziamento del terrorismo per molte ragioni. In primo luogo, possono consentire un maggiore anonimato rispetto ai tradizionali metodi di pagamento non in contanti. I sistemi di valuta virtuale possono essere scambiati su Internet, sono generalmente caratterizzati da rapporti non faccia a faccia con i clienti e possono consentire finanziamenti anonimi (finanziamenti in contanti o finanziamenti di terze parti tramite scambiatori virtuali che non identificano correttamente la fonte di finanziamento). Possono inoltre consentire trasferimenti anonimi, qualora mittente e destinatario non siano adeguatamente identificati.

I sistemi decentralizzati sono particolarmente vulnerabili ai rischi dell'anonimato. Ad esempio, in base alla progettazione, gli indirizzi Bitcoin, che fungono da account, non hanno nomi o altri identificativi del cliente allegati e il sistema non ha un server centrale o un fornitore di servizi. Il protocollo Bitcoin non richiede né fornisce identificazione e verifica dei partecipanti né genera registrazioni storiche di transazioni che sono necessariamente associate all'identità del mondo reale. Non esiste un organismo di supervisione centrale e nessun software antiriciclaggio attualmente disponibile per monitorare e identificare modelli di transazioni sospette. Le forze dell'ordine non possono prendere di mira una sede centrale o un'entità (amministratore) a fini investigativi o di sequestro di beni (sebbene le autorità possano prendere di mira singoli scambiatori per informazioni sui clienti che lo scambiatore potrebbe raccogliere). Offre quindi un livello di potenziale anonimato impossibile con le tradizionali carte di credito e debito o con i vecchi sistemi di pagamento online, come PayPal.

Allo stesso modo, la portata globale della valuta virtuale aumenta i suoi potenziali rischi AML/CFT (Anti-Money Laundering/Combating the Financing of Terrorism). I sistemi di valuta virtuale sono accessibili tramite Internet (anche tramite telefoni cellulari) e possono essere utilizzati per effettuare pagamenti transfrontalieri e trasferimenti di fondi. Inoltre, le valute virtuali si basano comunemente su infrastrutture complesse che coinvolgono diverse entità, spesso sparse in più paesi, per trasferire fondi o eseguire pagamenti. Questa segmentazione dei servizi significa che la responsabilità per la conformità e la supervisione/applicazione di AML/CFT (Anti-Money Laundering/Combating the Financing of Terrorism) potrebbe non essere chiara. Inoltre, i record dei clienti e delle transazioni possono essere detenuti da entità diverse, spesso in giurisdizioni diverse, rendendo più difficile l'accesso alle forze dell'ordine e alle autorità di regolamentazione. Questo problema è esacerbato dalla natura in rapida evoluzione della tecnologia e dei modelli di business decentralizzati della valuta virtuale, compreso il numero e i tipi/ruoli mutevoli dei partecipanti che forniscono servizi nei sistemi di pagamento in valuta virtuale. E, cosa importante, i componenti di un sistema di valuta virtuale possono trovarsi in giurisdizioni che non dispongono di adeguati controlli AML/CFT. I sistemi centralizzati di valuta virtuale potrebbero essere complici del riciclaggio di denaro e potrebbero cercare deliberatamente giurisdizioni con regimi AML/CFT (Anti-Money Laundering/Combating the Financing of Terrorism) deboli. Le valute virtuali convertibili decentralizzate che consentono transazioni anonime da persona a persona possono sembrare esistere in un universo digitale completamente fuori dalla portata di un determinato paese.

Di conseguenza, le persone che desiderano riciclare proventi criminali spesso si rivolgono a token crittografici e altre criptovalute per aiutarli nel movimento di tali proventi. La Società è a rischio come detentrice di altre criptovalute e token crittografici.

SEZIONE 3. VALUTAZIONE DEL RISCHIO AZIENDALE

Lo scopo della valutazione del rischio aziendale è di:

- Identificare i principali rischi affrontati dalla Società nelle sue operazioni quotidiane;
- Valutare la probabilità che ciascun rischio incida sulla Società;
- Valutare le procedure ei controlli in atto per mitigare questi rischi.

Dal punto di vista dell'AML, il rischio principale per la Società è l'avvio di una relazione commerciale (tramite la vendita, l'acquisto di metalli preziosi) che porta la Società a diventare coinvolta o associata a reati finanziari o attività terroristiche. Il potenziale impatto negativo di questo rischio è enorme sia dal punto di vista finanziario che operativo e potrebbe comportare danni reputazionali, perdita di clienti, azioni normative e sanzioni e lunghi procedimenti legali.

Esistono molti modi in cui la Società potrebbe essere coinvolta o associata a un reato finanziario, inclusi ma non limitati a:

1. Ricevere pagamenti dai proventi di reato sotto forma di valuta FIAT o Criptovalute;
2. Fornire servizi a noti criminali, terroristi o individui con attività commerciali sospette;
3. Consentire a persone o società sanzionate di aggirare il blocco dei beni o altre sanzioni consentendo il trasferimento di fondi attraverso la piattaforma della Società;
4. La ricezione di criptovalute e altri token crittografici che vengono quindi essenzialmente associati ai proventi del crimine;
5. Mancata identificazione di operazioni sospette;
6. Assistenza alla circolazione dei proventi di reato.

Il programma di conformità della Società contiene una valutazione e una documentazione dei rischi associati al riciclaggio di denaro, al finanziamento del terrorismo e al finanziamento della proliferazione nella propria attività, in modo da consentire all'azienda di concentrare le proprie risorse dove sono più necessarie per gestire i rischi entro il suo livello di accettazione.

3.1 VALUTAZIONE

Nell'effettuare una valutazione del rischio della propria attività, la Società ha tenuto conto degli elementi illustrati nelle Linee Guida.

Un approccio basato sul rischio ci consente di identificare potenziali rischi e indirizzare risorse e sforzi dove il rischio è maggiore e, al contrario, ridurre i requisiti dove il rischio è basso. La valutazione del rischio della Società registra i seguenti fattori:

3.1.1 I clienti del Banco Metalli, i possessori di Token che vengono utilizzati per l'acquisto del metallo prezioso in custodia e le relazioni commerciali;

3.1.1.1 Questi includono i rischi associati alle tipologie di clienti che instaurano un rapporto d'affari con il Banco Metalli. Esempi di categorie di clienti che possono indicare un rischio più elevato includono persone politicamente esposte (PEP), individui o società sanzionati, clienti la cui natura, struttura o relazione rendono difficile identificare il titolare effettivo finale di interessi significativi o di controllo, nonché come clienti che effettuano operazioni in circostanze insolite.

3.1.1.2 Esiste il rischio che le persone e le società soggette a sanzioni possano cercare di utilizzare i token come mezzo per aggirare le sanzioni per il congelamento dei beni attualmente in vigore. La Società dovrà garantire che tutti i titolari di Token o gli utenti della piattaforma collegata alla Società siano confrontati con gli elenchi pertinenti di individui e società sanzionati in modo da combattere tale abuso.

3.1.1.3 I possessori di Token possono, infatti, essere delegati di persone e società sanzionate e possono di fatto detenerli per conto di soggetti a cui è vietato farlo.

3.1.1.4 I prodotti e servizi della Società e i canali di consegna attraverso i quali li offre;

3.1.1.5 Questi includono i rischi associati ai tipi di prodotti e servizi offerti dalla Società (ossia i token) e al modo in cui tali prodotti e servizi vengono forniti ai clienti.

3.1.1.6 I Token e la piattaforma della Società potrebbero essere utilizzati come mezzo per finanziare il terrorismo o in altro modo finanziare persone, società o gruppi soggetti a sanzioni.

3.1.1.7 Le località geografiche in cui la Società svolge le proprie attività e le località geografiche dei propri clienti;

3.1.1.8 L'accettazione da parte della Società di altri token crittografici o criptovalute come mezzo di pagamento per i token;

3.1.1.9 L'accettazione da parte del Banco Metalli di token crittografici e criptovalute come asset del Banco Metalli;

3.1.1.10 Oltre a tutti i rischi di tracciabilità del denaro trasferito a mezzo bonifico bancario per la consistenza e la provenienza dei fondi utilizzati. Qualsiasi altro fattore rilevante relativo all'attività del Banco Metalli, ai suoi clienti e ai rapporti commerciali che ha con loro.

3.2 MISURE DI CONTROLLO

La gestione e la mitigazione dei rischi comporteranno:

- Applicazione di misure di adeguata verifica della clientela (KYC-KYB) per verificare l'identità dei clienti e di eventuali titolari effettivi che utilizzano i servizi di MyGold S.P.A.
- Ottenere informazioni aggiuntive o condurre una due diligence rafforzata sui clienti a rischio più elevato tramite piattaforme specializzate come ad esempio la piattaforma sumsub o direttamente dal Banco Metalli.
- Inoltre, il Banco Metalli si avvale di sistemi informatici come https://sumsub.com/crypto/ e https://gruppomit.com/software-antiriciclaggio/ per la gestione delle verifiche dei dati dei clienti a differenti livelli.
- Utilizzo dei servizi e dei database ufficiali nazionali e internazionali per controllare tutti i clienti e le transazioni per garantire che non siano Persone Politicamente Esposte o soggette a sanzioni.
- Screening dei Token holder al momento del riscatto per combattere il potenziale riciclaggio di denaro, inclusa l'identificazione e la segnalazione di eventuali transazioni sospette e il monitoraggio e il controllo delle donazioni a organizzazioni non governative.
- Robuste procedure di conservazione delle registrazioni.

Ogni potenziale cliente sarà considerato utilizzando un approccio basato sul rischio per garantire che vengano ottenute le misure appropriate e necessarie per ottenere informazioni sufficienti sull'identità del cliente e sulle attività commerciali.

Per quanto riguarda il rischio in un'ottica di riciclaggio o finanziamento al terrorismo, la Società opera in un contesto di rischio molto “BASSO”. Tuttavia, attraverso l'attuazione delle procedure antiriciclaggio (“AML”) e contrasto al finanziamento al terrorismo (“CFT”) e alle procedure di

proliferazione che la Società adotterà e metterà in atto, la Società cercherà di mitigare i rischi individuati.

Il Banco Metalli esaminerà periodicamente questa valutazione del rischio aziendale per assicurarsi che rimanga adeguata ai servizi che fornisce.

Considerazione: nel 100% dei casi, di clienti vengono registrati nella piattaforma o mediante la APP, vengono identificati mediante i Financial Advisor abilitati alla consulenza indipendente e vigilati dagli organi di controllo dei vari paesi. Pertanto, l'identificazione del cliente avviene prevalentemente in presenza, oltre ai processi interni che prevedono una chiamata dal nostro customer service ai clienti che si attivano per la prima volta.

Come Operatore professionale in Oro, MyGold S.P.A. è tenuta a sottostare ai seguenti adempimenti secondo norma di legge: Contrasto al terrorismo, Analisi operazioni sospette, Anagrafe Rapporti, Operazioni Extraconto, Deleghe Agenzia Entrate, Indagini Finanziarie Telematiche Agenzia Entrate, pertanto si avvale di software certificato per tali adempimenti

Il software è sviluppato da M.I.T. e consente alle società di tipo non finanziario di adempiere in maniera rapida ed efficiente agli obblighi previsti da L. 197/91, D.lgs. 56/2004, D.lgs. 231/2007 – Terza Direttiva.
Permette l'inserimento di prestazioni, sia pari o superiori ai 15.000,00 euro che frazionate, con controllo ed aggregazione automatica delle frazionate e contratti stipulati (definitivi e preliminari), sia pari che superiori ai 15.000,00 euro che frazionati, con controllo ed aggregazione automatica delle frazionate, ecc.
Sono già caricate tutte le codifiche richieste dall'UIF/Banca d'Italia necessarie per l'utilizzo del programma (Tipi di identificazioni, Tipo di finanziamento, ecc.).
Vengono gestite le anagrafiche dei clienti, con la gestione delle modifiche e delle cancellazioni, come da provvedimento UIF/Banca d'Italia.
È possibile gestire sia le anagrafiche che i contratti, in modalità provvisoria con scarico selezionato in definitivo.
Il software è automatizzato per gestire le seguenti operazioni e banche dati:

- Registrazione dei dati per Anagrafiche di soggetti, clienti e dei relativi titolari effettivi.
- Autovalutazione del rischio e adeguata verifica della clientela.
- Registrazione e conservazione di operazioni presso l'Archivio Unico Informatico (AUI).
- Comunicazioni all'Agenzia delle Entrate di dati anagrafici, saldi, movimenti e indagini finanziarie.
- Creazione di Segnalazioni Anti-Riciclaggio Aggregate (SARA) da inviare all'Unità di Informazione Finanziaria (UIF).
- Informazioni sui meccanismi transfrontalieri considerati potenzialmente aggressivi (DAC 6).

SEZIONE 4. QUADRO NORMATIVO

4.1 NORMATIVE

Molti paesi, comprese lo Stato Italiano, hanno emanato leggi per combattere il riciclaggio di denaro, il finanziamento del terrorismo, la proliferazione e il finanziamento della proliferazione. La legge delle dello Stato di Italia impone al Banco Metalli l'obbligo di monitorare le proprie attività per potenziali riciclaggio di denaro e/o finanziamento del terrorismo e impone sanzioni sostanziali in caso di non conformità. I nostri clienti e dipendenti dovrebbero essere fiduciosi che il Banco Metalli non solo amministra la propria attività nel pieno rispetto della legge, ma cerca anche attivamente di svolgere un ruolo positivo come buon cittadino aziendale per promuovere gli obiettivi alla base di questa legge.

Le società che operano come Banco Metalli sono soggetti alla legislazione e ai regolamenti dello Stato Italiano e a qualsiasi guida o regolamento di vigilanza pertinente promulgato dalla EU:

(1) Norme Anticorruzione
(2) Codice penale
(3) Proventi del diritto penale
(4) Legge sul terrorismo
(5) Legge sull'abuso di droghe
(6) Finanziamento della proliferazione (divieto)
(7) Normativa Antiriciclaggio
(8) Sanzioni e ordini finanziari mirati a livello internazionale
(9) Note di orientamento sulla prevenzione e l'individuazione del riciclaggio di denaro, del finanziamento del terrorismo

Sanzioni severe sono inflitte a chiunque non rispetti le politiche, le procedure e i controlli pertinenti o non segnali alcuna conoscenza, convinzione o sospetto che un'altra persona sia coinvolta in una condotta criminale o coinvolta nell'assistere o agevolare il riciclaggio di denaro. È quindi fondamentale che tutti i dipendenti comprendano e rispettino pienamente le proprie responsabilità legali.

4.2 I REATI SPECIFICI AI PROCEDIMENTI DEL DIRITTO PENALE

I tre principali reati di riciclaggio di denaro sono:

(a) Nascondere, mascherare, convertire, trasferire o rimuovere proprietà criminali;

(b) Essere coinvolti in un accordo sapendo o sospettando che faciliti l'acquisizione, la conservazione, l'uso o il controllo di proprietà criminali; o

(c) Acquisire, utilizzare o possedere proprietà criminali.

È anche reato tentare, cospirare, incitare, aiutare, favorire, consigliare o procurare la commissione di uno dei tre principali reati di riciclaggio di denaro.

Con il termine “comportamento criminale” si intende qualsiasi comportamento, ovunque esso avvenga, che possa costituire reato. Ciò include reati di traffico di droga, furto e frode, rapina,

contraffazione, prelievo illegale di depositi, ricatti ed estorsioni.

MANCATA SEGNALAZIONE

(d) Mancata Divulgazione (Dipendente)

Una persona commette un reato se sa o sospetta o ha ragionevoli motivi per sapere o sospettare che un'altra persona sia coinvolta in una condotta criminale e non fa la necessaria divulgazione a un funzionario nominato (MLRO) o all'Autorità di Vigilanza.

La legge tutela i dipendenti da azioni legali per violazione della riservatezza nei casi in cui il dipendente segnala il sospetto che una persona possa essere coinvolta in una condotta criminale se il dipendente agisce secondo le procedure pertinenti.

(e) Mancata Divulgazione (Funzionario Nominato)

Un funzionario nominato commette un reato se sa o sospetta o ha fondati motivi per sapere o sospettare che un'altra persona sia coinvolta in una condotta criminale, o se ha ricevuto informazioni a seguito di una divulgazione che gli è stata data che forniscono ragionevoli motivi per tale conoscenza o sospetto e non effettua la prescritta comunicazione all'Autorità di Vigilanza.

4.3 I REATI DELLA LEGGE ANTICORRUZZIONE ("ACL")

Ai sensi dell'ACL, è illegale per una persona corrompere un pubblico ufficiale del governo, un membro dell'Assemblea legislativa o un pubblico ufficiale straniero al fine di ottenere o mantenere un vantaggio nel corso degli affari, direttamente o indirettamente.

I reati specifici previsti dall'ACL sono:

(a) Corruzione di funzionari locali e stranieri (ossia persona che, direttamente o indirettamente, concede a un pubblico ufficiale o qualsiasi pubblico ufficiale sollecitando, accettando o ottenendo, o accettando di accettare o ottenere, per sé o per un'altra persona, qualsiasi prestito, ricompensa, vantaggio o beneficiare con l'intento di interferire con l'amministrazione della giustizia, procurare o facilitare la commissione di un reato o proteggere dall'individuazione o dalla punizione di un delinquente).
(b) Frode al governo.
(c) Abusi di Uffici Pubblici o Eletti.
(d) Commissioni Segrete.
(e) Segnalazione di reati (ossia mancata segnalazione alla Commissione da parte della persona alla quale è stato chiesto o ottenuto un beneficio e dichiarazioni mendaci alla Commissione qualora tali dichiarazioni siano note per essere false o intese a fuorviare o non coerenti con una precedente dichiarazione fatto in base a qualsiasi legge).
(f) Tentativo, cospirazione o istigazione a commettere corruzione.
(g) Favorire, favorire, consigliare o procurare commissioni di corruzione.
(h) Reato commesso con il consenso, connivenza o negligenza di un ufficiale.

4.4 NORMATIVA ANTIRICICLAGGIO

I regolamenti antiriciclaggio ("AML") richiedono a chiunque sia coinvolto in attività commerciali pertinenti di disporre di sistemi e formazione per rilevare e prevenire il riciclaggio di denaro.

In effetti, l'AML richiede alla Società di:

a) Mantenere le politiche, le procedure e i controlli interni basati sul rischio. Queste procedure includeranno:

   i. procedure per l'accertamento della vera identità del richiedente d'impresa (KYB-KYC);
   ii. procedure di controllo interno e di comunicazione eventualmente idonee al monitoraggio continuo dei rapporti commerciali o di un'operazione una tantum;
   iii. procedure a supporto del riconoscimento e della segnalazione di attività sospette;
   iv. la conservazione e il mantenimento dei registri per il periodo di tempo prescritto;
   v. procedure di screening dei dipendenti per garantire standard elevati di assunzione;
   vi. sistemi adeguati ad identificare il rischio in relazione a persone, paesi e attività che devono includere controlli rispetto a tutti gli elenchi di sanzioni applicabili;
   vii. procedure di gestione del rischio relative alle condizioni alle quali un cliente può utilizzare il rapporto commerciale prima della verifica.

b) Nominare un Compliance Officer Antiriciclaggio a livello dirigenziale con la responsabilità di monitorare e garantire il rispetto interno delle Leggi.
c) Intraprendere un programma di audit interno.
d) Assicurarsi che vi sia un programma di formazione AML del personale.

Le procedure contenute in questo manuale soddisfano i requisiti di cui sopra. Sono anche note collettivamente come procedure **Know Your Customer** ("KYC") o **Customer Due Diligence** ("CDD"). La violazione di queste procedure può esporre la Società a indagini normative ed esporre le persone (direttori, funzionari e personale) a procedimenti giudiziari.

4.5 ATTIVITÀ FINANZIARIE RILEVANTI

L'AML deve essere seguito da qualsiasi persona che conduca "**affari finanziari rilevanti**" ("RFB"). La cui condotta porta una persona nell'ambito dei regolamenti AML, comprende (tra le altre) attività regolamentate, come attività bancarie, attività fiduciarie, servizi societari/fiduciari, investimenti in titoli affari e affari di fondi regolamentati, gestione di criptovalute.

4.6 RESPONSABILITÀ ANTIRICICLAGGIO

Al fine di soddisfare i requisiti di conformità, stabiliti nell'AML, la Società ha nominato un Responsabile della conformità antiriciclaggio ("AMLCO"). L'alta dirigenza è responsabile del programma di conformità globale del Banco Metalli a tutti i requisiti legali e normativi internazionali e locali applicabili alla Società. L'alta dirigenza è responsabile della supervisione, selezione e monitoraggio dell'AMLCO. La Società si affida all'AMLCO, sotto la supervisione dell'alta dirigenza, per quanto segue:

- Sviluppo e mantenimento di sistemi e controlli (comprese politiche e procedure documentate) in linea con l'evoluzione dei requisiti;
- Garantisce audit regolari dei programmi AML/CFT;
- Fornisce consulenza al Consiglio in merito a questioni di conformità AML/CFT che devono essere portate alla sua attenzione;
- Riferisce periodicamente, se del caso, ai sistemi e ai controlli della Società.

Al momento della pubblicazione di questo manuale, l'AMLCO è Luca Canella.

ULTERIORI PROCEDIMENTI AML

Con il fine di aumentare la sicurezza che la gestione dei processi di controllo AML sono eseguiti correttamente, la Società ha affidato a consulenti esterni alcuni processi di secondo livello di verifica con il fine di garantire una maggiore affidabilità delle attività AML.

Alla stesura del presente manuale la gestione è stata affidata all'Impresa Prifinance.

SISTEMI OPERATIVI DI CONTROLLO INTERNO

La società si avvale di software esterni per autenticare le procedure di KYC e KYB delle persone che decidono di utilizzare il wallet di MYGOLD SPA.

La procedura pertanto prevede tre livelli di verifica:

- Livello 1 raccolta dati e gestione sulla piattaforma https://sumsub.com/crypto/
- Livello 2 trasmissione dei dati alla società esterna contrattata per eseguire ulteriori verifiche.
- Livello 3 verifica interne sugli esiti delle risposte del livello 1 e 2.

4.7 REATI AI SENSI DEL REGOLAMENTO

Se è accertato dalle autorità che un Exchange non sta mantenendo le proprie procedure antiriciclaggio in conformità con i regolamenti, potrebbe essere colpevole di un reato.

Ovviamente, alla luce di questi requisiti legali e regolamentari, non è solo il rischio reputazionale o finanziario per la Società che deve essere preso in considerazione, ma anche il rischio più personale qualora un dipendente della Società sia accusato o ritenuto coinvolto in attività criminali condurre o è a conoscenza di tale attività ma omette di segnalarla secondo tali procedure.

4.8 NORME SUL TERRORISMO

Le norme sul terrorismo contengono numerosi reati, sanzioni e difese associati ad attività legate al terrorismo, alla manipolazione di proprietà del terrorismo e al finanziamento del terrorismo.

SEZIONE 5. CONOSCI IL TUO CLIENTE – KYC-KYB

5.1 INTRODUZIONE

I termini KYC e due diligence sono usati in relazione all'antiriciclaggio ed entrambi sono usati globalmente per descrivere l'identificazione dei clienti e le procedure di verifica, che comprendono gli obblighi del Banco Metalli. Collettivamente e per gli scopi descritti nel presente manuale, entrambi questi termini comprendono i vari elementi e fasi necessari per acquisire nuovi clienti e rivedere i clienti esistenti.

Una panoramica generale dei requisiti di due diligence del KYC è contenuta in questo manuale. Nell'attuazione dei requisiti KYC, la Società si avvale dei tre livelli di sicurezza descritti in precedenza.

5.2 IDENTITÀ DEL CLIENTE

La legislazione richiede che il Banco Metalli garantisca che sia chiaro a chi vengono forniti i servizi e adottino "misure ragionevoli" per verificare l'identità di tutti i clienti.

All'interno della legislazione, dei regolamenti e del presente manuale, il cliente può essere indicato come il "richiedente". Le procedure KYC-KYB sono richieste per tutti i "richiedenti", che possono essere uno o più dei seguenti:

5.2.1 Il cliente diretto;
5.2.2 Il cliente finale;
5.2.3 Il beneficiario effettivo del cliente finale;
5.2.4 Un intermediario che agisce per conto del cliente finale.

Il rapporto con il cliente deve essere esaminato con molta attenzione e deve essere stabilito per chi sono richieste le procedure KYC-KYB, che possono essere più di un individuo o entità. Eventuali ambiguità o dubbi devono essere riferiti all'alta dirigenza e/o all'AMLCO/MLRO.

5.3 PROCEDURE DI IDENTIFICAZIONE DEL CLIENTE

Quando si considera l'avvio di una relazione d'affari, ci sono una serie di problemi che riguardano CDD:

- Stabilire l'identità del cliente;
- Verificare l'identità del cliente e assicurarsi che il cliente sia chi afferma di essere;
- Identificare chi può avere il controllo di una persona giuridica, persona giuridica o esercitare il controllo sulle risorse finanziarie del cliente;
- Comprendere la fonte di fondi/attività/ricchezza che saranno detenuti, trasferiti o controllati dal cliente incluso;
- Ottenere informazioni sufficienti sulla natura dell'attività per comprendere l'attività passata e futura del cliente, insieme a qualsiasi modello previsto o previsto di attività futura.

5.4 OBBLIGHI DI DOCUMENTAZIONE DEL CLIENTE E RENDICONTAZIONE

Conoscere il tuo cliente ("KYC") è essenziale nella lotta al riciclaggio di denaro.

Al fine di configurare un nuovo account, un potenziale cliente del Banco Metalli dovrà eseguire le seguenti operazioni per soddisfare le procedure AML e KYC della Società:

1. Ottenere una copia autenticata di un documento d'identità con foto emesso dal governo e una prova dell'indirizzo. Se possibile, la documentazione originale dovrebbe essere vista in un incontro faccia a faccia. Questi articoli possono essere sotto forma di patente di guida o passaporto, nonché di una bolletta, un contratto di noleggio, un contratto residenziale o una lettera del governo.

2. Condurre controlli di screening pertinenti tramite sistemi informatici (4stop interagisce con le maggiori piattaforme informatiche del mondo) per stabilire: identificazione, persone politicamente esposte, elenchi delle sanzioni applicabili, elenco dei cittadini appositamente designati e delle persone bloccate.

3. Assegna un livello di rischio in base alle circostanze e ai risultati sullo screening del database.

Poiché è probabile che eventuali problemi riscontrati in relazione al riciclaggio di denaro o alla condotta criminale si verifichino in futuro quando potrebbe essere difficile ricordare quale azione è stata intrapresa, è essenziale che le prove documentali e le registrazioni siano adeguatamente conservate. Fatte salve eventuali esenzioni o eccezioni applicabili, un file KYC del cliente separato conterrà tutte le informazioni e la documentazione a cui si fa riferimento in questo manuale.

5.5 QUANDO DEVE ESSERE IDENTIFICATA L'IDENTITÀ?

È buona norma confermare l'identità e/o la proprietà prima di dare accesso al conto deposito con piena funzionalità. Resta in ogni caso attivo un'allerta di sistema. In questi casi possono essere richieste ulteriori documenti che autenticano la legittimità dell'operazione.

Qualora un cliente non fornisca documentazione adeguata, si dovrebbe prendere in considerazione la risoluzione del rapporto e se debba essere presentata una segnalazione di attività sospetta.

5.6 VERIFICA DELLA DOCUMENTAZIONE

Ove possibile, i documenti ricevuti dovrebbero essere verificati in modo indipendente per stabilirne l'autenticità e la legittimità.

Tutti i documenti devono essere validi e aggiornati e se un documento contiene una data di scadenza, come un passaporto, è necessario verificare che la data di scadenza non sia trascorsa. I documenti che scadono in futuro dovrebbero essere rinnovati ogni volta che se ne presenta l'opportunità. Tuttavia, nei casi in cui vi siano informazioni sufficienti per indicare che l'identificazione del cliente può essere prontamente verificata con altri mezzi (come informazioni recenti su Internet) e la valutazione del rischio non è elevata, potrebbe non essere necessario aggiornare la documentazione scaduta. Dovrebbe essere fatta una nota di archivio che rifletta la giustificazione di tale decisione.

I passaporti e altre prove documentali dovrebbero apparire familiari e avere l'aspetto di altri documenti comparabili ricevuti da altri clienti. Nel caso in cui un documento sollevi dubbi sulla sua autenticità, è necessario rivolgersi immediatamente all'alta dirigenza e/o all'AMLCO.

Va notato che i criminali falsificano documenti, che potrebbero non essere immediatamente evidenti come fraudolenti. Nella misura del possibile, il personale è tenuto a utilizzare il proprio miglior giudizio

e ad adottare misure ragionevoli per stabilire che i documenti siano riconoscibili e appaiano legittimi.

Un approccio basato sul buon senso e sul rischio dovrebbe essere adottato in relazione alla documentazione di due diligence poiché le persone di alcuni paesi potrebbero avere difficoltà a fornire documenti che corrispondano esattamente a questi requisiti. In caso di problemi in relazione alla documentazione di identificazione, fare riferimento alle Note di orientamento per ulteriori consigli.

5.7 CERTIFICAZIONE DELLA DOCUMENTAZIONE

Il sistema, raccolti i documenti, attiva i processi di validazioni previsti dalla procedura.

Il livello uno è il controllo eseguito dall'operatore che determina se validare o meno l'attivazione del conto deposito.

Lo stesso operatore recupera le informazioni dalla piattaforma 4stop, e le confronta per valutare se vi sono le condizioni di attivazione e validazione della documentazione. Se tutti gli indicatori sono verdi, l'operatore abilita il conto deposito del cliente.

Le stesse informazioni sono trattate dalla società esterna per un ulteriore verifica sull'utente che ha richiesto l'uso del conto deposito a MyGOLD SpA.

5.8 APPROCCIO BASATO SUL RISCHIO

È importante che i dirigenti e il personale della Società adottino e attuino le politiche contenute in questo manuale.

Un approccio basato sul rischio è uno dei modi più efficaci per proteggersi dal riciclaggio di denaro. È essenziale comprendere che alcuni rischi associati ai vari elementi del profilo di un cliente possono essere indicativi di potenziali attività criminali, come questioni geografiche e giurisdizionali, tipi di attività e prodotti, canali di distribuzione e tipi e importi di transazione prevalenti.

I clienti saranno esaminati, valutati e allocati con un livello appropriato di rischio di riciclaggio di denaro. I clienti saranno designati come ad alto, medio o basso rischio.

5.8.1 **Il cliente ad alto rischio** sarà soggetto a livelli avanzati di due diligence che vanno al di là delle politiche e dei principi fondamentali contenuti in questo manuale;

5.8.2 **I clienti a rischio medio** saranno soggetti alle politiche e procedure fondamentali contenute nel presente manuale;

5.8.3 **I clienti a basso rischio** possono essere soggetti a una certa flessibilità all'interno delle politiche e delle procedure contenute in questo manuale, tuttavia, è necessario prestare grande attenzione per garantire che la Società continui a adempiere ai propri obblighi legali.

Sebbene sia accettato che la mancata presentazione di una documentazione di due diligence soddisfacente possa essere indicativa di un problema di riciclaggio di denaro, si riconosce anche che, a causa della diversità geografica delle attività finanziarie, a volte potrebbe rivelarsi difficile o impossibile ottenere una documentazione che soddisfi esattamente i criteri stabiliti in questo manuale.

Se si verifica questa situazione e non vi sono motivi per sospettare di riciclaggio di denaro, la documentazione del cliente deve essere trasmessa all'alta dirigenza e/o all'AMLCO, insieme a una

spiegazione del tipo di problemi sorti. L'alta dirigenza, in consultazione con l'AMLCO, esaminerà la documentazione e considererà i rischi associati all'accettazione di prove di identificazione che non rientrano in queste procedure, in seguito, fornendo al personale, consulenza e guida a seconda dei casi. I rischi considerati nel processo di valutazione e decisione e le conclusioni raggiunte dovrebbero essere adeguatamente documentati per il file KYC del cliente, con l'appropriata approvazione da parte delle persone coinvolte. Solo l'alta dirigenza, in consultazione con l'AMLCO o l'MLRO, può determinare il livello di rischio elevato da attribuire a un particolare cliente o approvare la documentazione che non soddisfa i requisiti esatti della politica antiriciclaggio della Società.

Tutti i clienti sono soggetti a una valutazione del rischio in modo che i probabili livelli di monitoraggio futuri siano anticipati e ragionevoli. Le valutazioni del rischio saranno registrate nel file. I requisiti di due diligence e il monitoraggio futuro pianificato devono essere commisurati al livello di rischio associato al cliente e sarà necessaria una due diligence rafforzata per tutti i clienti a rischio più elevato.

5.9 SCREENING DEL DATABASE

La Società utilizzerà un database di intelligence altamente strutturato che contiene i nomi di noti criminali come riciclatori di denaro, terroristi, truffatori, persone registrate su "liste nere" governative, ecc. Insieme ai profili dei paesi di giurisdizioni note per alti livelli di attività criminale. Inoltre, tali database contengono i nomi delle Persone Politicamente Esposte (PEP), per i quali ulteriori dettagli possono essere trovati nelle seguenti sezioni di questo manuale.

La Società esaminerà ogni nuovo cliente (tutti i soggetti rilevanti) rispetto a un database riconosciuto nell'ambito del processo di identificazione al momento della ricezione della richiesta di servizi e successivamente periodicamente. Attraverso questo database, tutti i clienti saranno sottoposti a screening rispetto agli elenchi di sanzioni applicabili per garantire che le attività non siano condotte con paesi interessati da sanzioni imposte dall'UE (Unione Europea) ONU (Nazioni Unite) o OFAC (Office of Foreign Assets Control) che include l'Elenco dei cittadini appositamente designati (SDN) e Elenco delle persone bloccate.

L'ulteriore azione richiesta dipenderà dai risultati dello screening, tuttavia l'alta dirigenza e/o l'AMLCO dovranno essere informati di qualsiasi "risultato" sul database che richieda la considerazione per designare il cliente come ad alto rischio.

5.10 CLIENTI AD ALTO RISCHIO

Un cliente ad alto rischio sarà colui che presenta un rischio negativo superiore al normale di coinvolgimento nel riciclaggio di denaro o genera problemi relativi ai requisiti di riciclaggio di denaro o qualsiasi altra questione che l'alta dirigenza o l'AMLCO considerano significativa.

Al fine di mitigare i rischi associati ai clienti ad alto rischio, sarà necessario considerare l'applicazione di un livello di due diligence rafforzata per tali clienti in termini di approvazione iniziale e monitoraggio continuo. L'alta dirigenza, in consultazione con l'AMLCO, determinerà se il livello di rischio è accettabile.

La due diligence rafforzata ("EDD") dovrà andare oltre i normali requisiti applicati all'approvazione e al monitoraggio dei clienti, come contenuti nel presente manuale. Poiché i motivi per la designazione come ad alto rischio variano da cliente a cliente, la natura e il livello di miglioramento dovranno essere determinati separatamente man mano che i clienti ad alto rischio verranno identificati e le procedure dovranno spiegare come ridurre al minimo l'aumento dei rischi.

Qualora si accerti che un cliente che soddisfa i criteri per la designazione ad alto rischio non giustifica una due diligence rafforzata, i motivi della decisione e il modo in cui i rischi sono mitigati dovrebbero comunque essere pienamente documentati e inseriti nel fascicolo del cliente.

Inoltre, tutte le procedure EDD eseguite durante il processo di approvazione, insieme alle procedure proposte per il monitoraggio futuro, dovrebbero essere completamente documentate e inserite nella pratica del cliente. Nel caso in cui in futuro si dovessero riscontrare problemi quando il personale potesse non ricordare prontamente i passi intrapresi, la Società sarà in grado di fornire evidenza della due diligence svolta a suo tempo e fornire la motivazione per la proposta monitoraggio continuo.

Le migliori pratiche internazionali raccomandano di prestare particolare attenzione alle seguenti questioni:

- Paesi ad alto rischio;
- Persone politicamente esposte ("PEP");
- Imprese attraenti o soggette a riciclaggio di denaro.

Tutte le relazioni ad alto rischio saranno registrate ai fini della segnalazione e del monitoraggio.

5.11 PAESI AD ALTO RISCHIO E NON CONFORMI

Alcuni paesi sono associati a reati presupposto di riciclaggio di denaro come traffico di droga, frode e corruzione e, di conseguenza, rappresentano un rischio potenziale maggiore per la Società. La conduzione di un rapporto d'affari con persone di tale paese può esporre la Società a maggiori rischi reputazionali e legali.

Particolare attenzione dovrebbe essere data ai paesi:

5.11.1 senza strategie antiriciclaggio efficaci o equivalenti;
5.11.2 dove il contante è il mezzo di scambio prevalente e normale;
5.11.3 instabilità politica e/o alti livelli di corruzione nel settore pubblico o privato;
5.11.4 paesi noti di transito o traffico di droga.

La Società consulterà i database disponibili al pubblico o eventuali elenchi pubblicati dalla FIU e stabilirà se i collegamenti dei clienti con i paesi elencati giustifichino la valutazione del cliente come ad alto rischio. Dovrebbe essere preso in considerazione il modo in cui i rischi prevalenti possono essere mitigati conducendo una due diligence aggiuntiva e più dettagliata. Occorre prestare attenzione quando si accettano documenti di identificazione, in particolare documenti in copia certificata, provenienti da paesi ad alto rischio o non conformi.

5.12 PERSONE POLITICAMENTE ESPOSTE (“PEP”)

Una persona politicamente esposta o PEP è un termine utilizzato per descrivere una persona che ricopre una posizione pubblica che potrebbe essere esposta alla corruzione. Il seguente elenco contiene esempi di persone che possono essere considerate PEP, sebbene questo elenco non debba essere considerato esaustivo:

5.12.1 Capo di Stato;
5.12.2 Ministri e politici di governo;
5.12.3 Funzionari pubblici influenti;
5.12.4 Giudici;

5.12.5 Comandanti militari e alti ufficiali militari;
5.12.6 Familiari o stretti collaboratori di uno qualsiasi dei suddetti;
5.12.7 Partner commerciali o collegamenti aziendali di uno qualsiasi dei precedenti.

Viene creato un rischio negativo per i PEP in quanto potrebbero utilizzare la loro posizione pubblica o scoprire che la loro posizione pubblica viene inconsapevolmente utilizzata, a proprio vantaggio personale o a beneficio di altri che potrebbero essere coinvolti in attività illegali come corruzione, concussione e frode.

I PEP presentano un rischio reputazionale considerevole per un fornitore di servizi finanziari se si scopre che tale istituto è coinvolto con un funzionario pubblico che abusa della sua posizione. Il rischio avverso aumenta considerevolmente quando un PEP si trova in un paese ad alto rischio.

La Società garantirà che ogni titolare effettivo o titolare del trattamento sottostante non sia un PEP eseguendo ricerche su database ufficiali nazionali e internazionali per schermare i nomi rispetto al proprio database o facendo riferimento a informazioni pubblicamente disponibili. I risultati di tale verifica saranno registrati. Nel caso in cui venga identificato un PEP, la Società:

A. Assegna al cliente un rating di alto rischio;
B. Completare il PEP Report, assicurando che l'Alta Direzione e il consiglio di amministrazione approvi la creazione di un'attività con il cliente;
C. Condurre una due diligence rafforzata ed essere vigili nel monitorare il rapporto commerciale;
D. Garantire che saranno adottate misure ragionevoli per stabilire la fonte di ricchezza e la fonte di fondi;
E. Le relazioni PEP saranno tracciate in View Point ai fini della segnalazione e del monitoraggio.

5.13 INDIVIDUI ED ENTITÀ SANZIONATE

Quando si valuta l'accettazione di nuovi clienti, è necessario prestare attenzione per garantire che la Società non conduca affari con paesi interessati da sanzioni imposte dall'UE (Unione Europea) ONU (Nazioni Unite) o OFAC (Office of Foreign Assets Control) a seguito di accettare quel nuovo affare.

Ai sensi della Legge sui proventi di reato, della Normativa Antiriciclaggio e della Legge sul Terrorismo, la Società è tenuta a sporgere denuncia di attività sospetta all'Autorità preposta alla redazione dei documenti contabili societari nel caso in cui venga scoperto un rapporto che contravviene ad un provvedimento sanzionatorio o ad una disposizione di Legge.

La Società deve documentare e registrare tutte le azioni intraprese per ottemperare al regime sanzionatorio e la motivazione di tale azione. L'alta dirigenza, in consultazione con l'AMCLO, valuterà se sono necessarie ulteriori azioni come il congelamento dei fondi e/o l'informazione delle autorità come richiesto dalle leggi pertinenti.

Tutti i soggetti/entità identificati nell'eventuale elenco sanzionatorio saranno registrati ai fini della segnalazione e del monitoraggio.

SEZIONE 6. PROCEDURE DI IDENTIFICAZIONE

6.1 PROCESSO DI IDENTIFICAZIONE E VERIFICA

Il processo di identificazione e verifica viene eseguito su tutti gli utenti che decidono di accedere al conto deposito di MYGOLD SpA.

6.2 VERIFICA DEL CLIENTE

La seguente documentazione deve essere ottenuta per verificare i clienti:

6.2.1 INDIVIDUALI/DIRETTORI/AMMINISTRATORI (può essere più di uno)

A. Le seguenti informazioni sono richieste per tutti i ***singoli*** clienti:

- Nome/nomi completi utilizzati;
- Indirizzo permanente corretto, compreso il codice postale (se appropriato);
- Data e luogo di nascita;
- Nazionalità;
- Occupazione;
- Scopo/natura dell'attività prevista;
- La fonte dei fondi (ovvero, generata da una transazione o da un'attività).

B. Identificazione con foto: ottenere ***una*** copia autenticata o autenticata di un documento che stabilisca l'identità della persona. Ciò può includere:

- Passaporto;
- Patente di guida con foto con firma;
- Identificazione delle Forze Armate;
- Un altro documento d'identità rilasciato dal governo.

C. Prova dell'indirizzo: ottenere ***una*** copia autenticata o autenticata di un documento che stabilisca l'indirizzo di residenza della persona. Ciò ***può*** includere:

- Bolletta delle utenze recenti (non più vecchia di tre mesi);
- Referenza di rispettato professionista che conosce il cliente;
- Copia del contratto di lavoro o conferma scritta del banchiere o del datore di lavoro.

6.2.2 IMPRESE

I seguenti documenti aziendali comprenderanno anche la documentazione di due diligence per una società:

- Certificato di costituzione;
- Certificato di cambio nome, se presente;

- Certificato di Good Standing (datato entro 6 mesi precedenti), se esistente;
- Nome e indirizzo della Sede Legale, se non Società;
- Nome e indirizzo di qualsiasi altro luogo di attività;
- Registro dei Soci/Azionisti;
- Albo degli Amministratori e dei Funzionari;
- Procure, se presenti;
- Atto costitutivo e Statuto;
- Delibera del Consiglio di Amministrazione di approvazione dell'ingresso nel rapporto con la Società.

SEZIONE 7. MONITORAGGIO

7.1 REQUISITI DI MONITORAGGIO

Una volta completate le procedure di identificazione e la Società ha instaurato un rapporto con il cliente, la Società deve continuare a monitorare la struttura del cliente e qualsiasi attività, se evidente, per assicurarne la coerenza con le aspettative e l'aggiornamento della documentazione di due diligence e in linea con le attuali esigenze. La frequenza e la natura dei processi di monitoraggio dipenderanno dal tipo di cliente, dall'attività svolta e dalla classificazione di rischio assegnata al cliente.

7.2 AREE DI MONITORAGGIO

I tipi di problemi che dovrebbero essere esaminati includono:

- Operazioni al riscatto dei Token e dei destinatari previsti;
- Cambiamenti nella struttura del cliente, nei rapporti commerciali, ecc.;
- Cambiamenti nelle persone inclusi amministratori, funzionari, persone autorizzate ecc.;
- Giurisdizioni in cui il cliente ha sede o svolge attività;
- Le aspettative sono state soddisfatte;
- Eventuali problemi considerati insoliti.

La motivazione di qualsiasi cambiamento nella struttura o nelle aspettative dovrebbe essere rivista e studiata fino al raggiungimento di un livello di soddisfazione accettabile. Se non è possibile raggiungere la piena soddisfazione, il cliente dovrebbe essere sottoposto a procedure di due diligence rafforzate, che potrebbero includere l'aumento della frequenza del processo di monitoraggio dei clienti.

7.3 REVISIONI PERIODICHE

La Società effettuerà periodicamente una revisione delle informazioni, attività e transazioni CDD e ricerche su Internet (collettivamente, la "Revisione periodica") per tutti i clienti. La frequenza della revisione sarà basata sulla valutazione del rischio: i clienti ad alto rischio saranno rivisti annualmente; I clienti a rischio medio ogni 2 anni e i clienti a basso rischio verranno rivisti ogni tre anni. L'obiettivo della Revisione Periodica è:

- Garantire che l'attività del cliente sia conforme alle informazioni dichiarate al momento dell'instaurazione del rapporto. (es. stato della licenza, volume di attività, ecc.).
- Garantire che la documentazione di due diligence rimanga adeguata.
- Garantire che la valutazione del rischio rimanga adeguata.

I risultati della revisione periodica saranno documentati per ciascuna entità e inseriti negli archivi del cliente.

SEZIONE 8. CONSERVAZIONE DELLA DOCUMENTAZIONE

8.1 REQUISITI PER LA CONSERVAZIONE DELLA DOCUMENTAZIONE

La Società è tenuta a conservare i registri relativi all'identificazione e alle transazioni dei clienti e altri atti che attengono a procedure antiriciclaggio.

La documentazione di due diligence potrebbe includere:

- Prove identificative;
- Qualsiasi altra due diligence raccolta durante l'assunzione e il monitoraggio del cliente;
- Dettagli ed estratti conto delle transazioni finanziarie;
- Note sugli archivi, verbali e altri record relativi all'attività del cliente;
- Nuovi record di approvazione commerciale, inclusi elenchi di controllo di due diligence e qualsiasi supporto documentale.

Inoltre, devono essere conservate le seguenti registrazioni:

- Registri di formazione, registri di test e piani;
- Segnalazioni di attività sospette ("SAR") e documentazione di accompagnamento;
- Registro delle Richieste contenente richieste rivolte o ricevute;
- Record di monitoraggio di conformità e MLRO.

La Società assicurerà che siano predisposte adeguate salvaguardie sulla riservatezza e sull'uso di informazioni scambiate durante la condivisione delle informazioni richieste per la due diligence e il rischio AML/CFT gestione all'interno del gruppo di società.

8.2 PERIODO DI CONSERVAZIONE DEI REGISTRI

Le registrazioni devono essere conservate per un minimo di 8 anni dalla data di chiusura del cliente o dopo la fine di un'eventuale indagine sul riciclaggio di denaro.

8.3 DISTRUZIONE DEI REGISTRI

Il personale deve contattare il senior management prima di distruggere i registri dei clienti. I registri non possono essere distrutti senza l'approvazione scritta dell'alta direzione, che confermerà il nome del cliente, la natura dei registri da distruggere e le loro date (ad esempio, data di chiusura e data di distruzione consentita).

Il Responsabile antiriciclaggio verificherà se è in corso o è mai stata in corso un'indagine per riciclaggio di denaro. Il Responsabile antiriciclaggio darà l'approvazione per la distruzione dei registri se non è stata presentata alcuna denuncia e se non c'è un'indagine in corso sul riciclaggio di denaro negli ultimi 5 anni.

È essenziale che tutta la documentazione, compresi i controlli e le autorità di approvazione, relativa alla distruzione dei registri sia documentata e conservata in archivio. Qualsiasi conferma deve anche essere ricevuta per iscritto e inserita nel file del rapporto.

SEZIONE 9. FORMAZIONE

9.1 FORMAZIONE AML INTRODUTTIVA

Nell'ambito della formazione introduttiva, tutti i nuovi dipendenti riceveranno una formazione antiriciclaggio.

I dipendenti permanenti e temporanei dovrebbero essere formati allo stesso modo, tenendo conto dell'ambito di applicazione di lavoro che potrebbe essere assegnato a un lavoratore interinale.

I nuovi dipendenti dovrebbero essere intervistati per accertare l'attuale livello di comprensione del riciclaggio di denaro.

Come minimo, ai nuovi dipendenti dovrebbero essere forniti:

- Accesso al Manuale di Conformità Antiriciclaggio della Società;
- Spiegazione degli obblighi di antiriciclaggio di un individuo;
- Identità e ubicazione di MLRO e DMLRO;

9.2 FORMAZIONE ANNUALE OBBLIGATORIA IN AML

Tutto il personale è tenuto a frequentare almeno una volta all'anno un corso di formazione in materia di antiriciclaggio. Tutti gli impiegati che partecipano a questi corsi di formazione annuali in materia di antiriciclaggio dovrebbero produrre prove del completamento della formazione da parte di tramite un certificato o una copia della registrazione all'AMLCO come prova che le persone hanno partecipato.

Pertanto, tutto il personale, indipendentemente dal livello di anzianità, dovrà partecipare a una formazione antiriciclaggio sessione almeno una volta all'anno.

SEZIONE 10. SEGNALAZIONE DI ATTIVITÀ SOSPETTE

Principali reati di riciclaggio di denaro

I principali reati di riciclaggio di denaro sono i seguenti reati contenuti nella legge sui proventi di reato (ma reati equivalenti sono contenuti nelle altre leggi del regime antiriciclaggio):

- Accordi relativi alla proprietà criminale: stipulare o essere coinvolti in un accordo che la persona conosce o sospetta, facilita l'acquisizione, la conservazione, l'uso o il controllo di proprietà criminale da parte o per conto di un'altra persona;
- Possesso di beni criminali: acquisire, utilizzare o avere possesso di beni criminali;
- Occultamento di proprietà criminali: occultamento, dissimulazione, conversione, trasferimento di proprietà criminali o rimozione dall'Italia. Tieni presente che nascondere o dissimulare proprietà criminali include nascondere o mascherare la sua natura, fonte, ubicazione, disposizione, movimento o proprietà o qualsiasi diritto ad essa relativo.
- Mancata segnalazione di un sospetto: una persona commetterà un reato se:

    - Sa o sospetta, o ha fondati motivi per sapere o sospettare che un'altra persona sia coinvolta in una condotta criminale;
    - Le informazioni su cui si basano le sue conoscenze o sospetti gli sono pervenute nel corso di un'attività regolamentata (o come risultato di una relazione interna nel caso dell'MLRO); e
    - Non effettua la divulgazione richiesta all'MLRO in merito alla persona e ai beni coinvolti nella sospetta condotta criminale o, nel caso dell'MLRO, alla FRA, non appena possibile dopo che le informazioni gli sono pervenute.

- Tipping Off: una persona commette il reato di "tipping off" se rivela che è stata effettuata (o sarà effettuata una segnalazione di attività sospetta), che è in corso (o proposta) un'indagine di polizia o che è stato effettuato l'accesso a ordini di informazioni fatto o ricercato, e sa che questa divulgazione potrebbe pregiudicare un'indagine.

10.1 REQUISITI DI SEGNALAZIONE DI ATTIVITÀ SOSPETTE

È responsabilità di tutti identificare i rischi di riciclaggio e di condotta criminale e, per farlo, devono sapere come identificare le attività sospette, che sono tipicamente il primo indicatore di riciclaggio. Inoltre, è mandato di tutti i dipendenti segnalare queste attività all'MLRO.

10.2 ATTIVITÀ INSOLITA E SOSPETTA

L'attività insolita è quella che non è coerente con l'attività nota o prevista del cliente o è anormale per il tipo di cliente o struttura. La chiave per identificare un'attività insolita è sapere abbastanza su un particolare cliente e sulla sua normale attività per essere in grado di riconoscere qualcosa di insolito. Esiste un'importante distinzione tra attività considerate insolite e attività ritenute, o note per essere, connesse a condotte criminali, riciclaggio di denaro o finanziamento del terrorismo.

A volte il personale della Società può imbattersi in attività o comportamenti ritenuti inusuali e non coerenti con le aspettative. L'attività insolita dovrebbe essere studiata, insieme con il cliente, il personale della Società e, se del caso, il MLRO.

Se i risultati delle indagini raggiungono una conclusione soddisfacente e non vi sono conoscenze, sospetti o ragionevoli motivi per sospettare una condotta criminale, non è necessario presentare una segnalazione interna.

Tuttavia, se le indagini portano alla conclusione che vi sono conoscenze, sospetti o fondati motivi per sospettare una condotta criminale o di riciclaggio di denaro, l'attività non solo è insolita, ma ora è anche considerata sospetta. In tali casi, una segnalazione interna deve essere presentata all'MLRO non appena ragionevolmente possibile.

10.3 PRESENTAZIONE DI UNA SEGNALAZIONE DI ATTIVITÀ SOSPETTA

I membri del personale sono tenuti a segnalare qualsiasi sospetto di condotta criminale direttamente all'MLRO il prima possibile. La relazione deve essere redatta per iscritto.

Una volta stabilito che l'attività è sospetta, non è necessario effettuare ulteriori indagini con il cliente e il cliente non deve mai essere informato che qualcuno ritiene che la sua attività sia sospetta né che è stata o sarà presentata una segnalazione.

Avvisare il cliente di un sospetto di riciclaggio di denaro è noto come 'tipping off, che è un reato penale che attira sanzioni pecuniarie e detentive. L'MLRO fornirà consulenza e guida qualora si presenti la necessità di trattare con il cliente e/o rispondere alle richieste del cliente.

Una volta che una segnalazione è stata presentata per un particolare cliente, il personale dovrebbe essere attento a qualsiasi attività aggiuntiva o contatto con il cliente. Anche se attività aggiuntive potrebbero non sembrare di per sé sospette, il personale dovrebbe tenere presente che le informazioni aggiuntive potrebbero aiutare l'organo di vigilanza sulle indagini. Pertanto, un'ulteriore segnalazione interna verrà solitamente depositata presso l'MLRO per qualsiasi attività aggiuntiva, e deciderà quindi se presentare nuovamente all'organo di vigilanza le informazioni ricevute.

Eventuali dubbi relativi ad attività sospette devono essere segnalati immediatamente all'MLRO.

10.4 RESPONSABILITÀ MLRO

Al ricevimento di una segnalazione da parte del personale della Società, l'MLRO:

- Firmare il rapporto e confermare la ricezione per iscritto alla persona interessata;
- Valutare se la segnalazione è stata depositata tempestivamente;
- Mettere una copia del rapporto e della ricevuta nel file interno;
- Valutare il rapporto e le prove a sostegno per determinare la linea d'azione richiesta;
- Considerare la politica e le procedure della Società, la legislazione, i regolamenti, le Note di orientamento e qualsiasi altro sviluppo applicabile.

Se l'MLRO concorda sul fatto che l'attività dà adito a un sospetto di riciclaggio di denaro, allora il MLRO:

- Presentare una segnalazione esterno all'Organo di Vigilanza non appena possibile;
- Inserire una copia della denuncia nel file interno;
- Valutare se la relazione debba continuare;

- Consigliare ai membri del personale coinvolti come procedere.

A seconda della natura dell'attività sospetta, l'MLRO deve decidere se raccomandare che il rapporto d'affari continui. Dovrebbe essere presa in considerazione anche l'ulteriore conduzione indagini e/o risoluzione del rapporto.

È necessario prestare attenzione per garantire che il cliente non sia avvisato della segnalazione o dei sospetti. In circostanze gravi, l'MLRO può consultare l'alta dirigenza su come procedere. Se si decide che il rapporto non deve continuare, è necessario prestare estrema attenzione nella notifica al cliente per assicurarsi che non venga inavvertitamente "informato" che è stata presentata una segnalazione.

Se l'MLRO non è d'accordo sul fatto che l'attività sia sospetta, l'MLRO:

- Determinare il motivo alla base di tale decisione;
- Documentare il motivo sulla segnalazione o allegare documentazione alla segnalazione.

10.5 REGISTRO DELLE SEGNALAZIONI

Tutte le attività relative ad una segnalazione devono essere gestite dall'operatore, via mail e registrate nel file dell'utente nel sistema informatico centrale indicando la data di invio della mail al MLRO il contenuto della segnalazione.

Questa modalità consente di avere uno storico delle segnalazioni per ogni cliente direttamente registrato a sistema.

SEZIONE 11. FUNZIONE DI AUDIT INTERNO

È un requisito delle normative antiriciclaggio che tutte le borse conducano regolarmente un audit AML/CFT. L'alta dirigenza ha la responsabilità di garantire che un audit interno sia condotto almeno una volta ogni tre anni.

11.1 COMPONENTI DELL'AUDIT INTERNO

I seguenti elementi saranno inclusi nell'audit AML/CFT della Società:

- attestare la complessiva integrità ed efficacia dei sistemi e dei controlli AM/CFT;
- valutare i propri rischi ed esposizioni rispetto a dimensione, linee di business, base clienti e ubicazione geografica;
- valutare l'adeguatezza delle politiche e delle procedure interne, tra cui l'identificazione e la verifica del Cliente, il mantenimento e la conservazione dei registri, i rapporti di affidamento e la documentazione di supporto e il monitoraggio delle Transazioni;
- verificare la conformità alle leggi e ai regolamenti in materia;
- testare le operazioni in tutte le aree della Società, con particolare attenzione alle aree, prodotti e servizi ad alto rischio;
- valutare la conoscenza da parte dei dipendenti di leggi, regolamenti, linee guida e politiche e procedure;
- valutare l'adeguatezza, l'accuratezza e la completezza dei programmi di formazione; e
- valutare l'adeguatezza del processo aziendale di identificazione delle attività sospette.

SEZIONE 12. CONOSCI IL TUO DIPENDENTE

L'alta dirigenza è responsabile di garantire che le procedure per l'assunzione e la verifica del personale richiedano che vengano effettuati controlli sufficienti sul background di un potenziale membro del personale prima di essere assunto. La Società condurrà una o più delle seguenti attività:

- verificare l'identità e il background del potenziale membro del personale;
- revisione dell'istruzione e dell'esperienza lavorativa;
- verificare le qualifiche professionali;
- verificare riferimenti e documenti giustificativi;
- gestire i nomi dei dipendenti attraverso un database di screening AML;
- eseguire tutte le altre misure di due diligence eventualmente necessarie (es. ricerca su Internet).

SEZIONE 13. POLITICA ANTICORRUZIONE

Le leggi della maggior parte dei paesi considerano il pagamento o l'offerta di pagamento o anche la ricezione di tangenti, bustarelle o altri pagamenti corruttivi un reato che potrebbe esporre la Società e i singoli dipendenti a sanzioni pecuniarie e/o detentive. Queste leggi anticorruzione rendono un reato pagare, offrire o dare qualsiasi cosa di valore a funzionari governativi stranieri, un partito politico straniero (o funzionario dello stesso) o candidati a cariche estere, allo scopo di influenzare gli atti o le decisioni di tali funzionari, partiti o candidati.

La Società si impegna a condurre la propria attività con onestà e integrità e nel rispetto delle leggi di tutti i paesi in cui la Società opera. Ciò include il rispetto di tutte le leggi, nazionali ed estere, che vietano pagamenti o incentivi impropri a qualsiasi persona, compresi i funzionari pubblici.

13.1 DICHIARAZIONE DELLA POLITICA

Il personale non deve consentire alcun uso dei fondi o di altri beni della Società per qualsiasi uso illecito o improprio.

Il personale non deve fare, né autorizzare nessuno a fare per conto della Società o ricevere, prestiti, ricompense, vantaggi o pagamenti di benefici o regali o offerte o promesse di pagare denaro o dare qualcosa di valore a o a beneficio di qualsiasi persona, o organizzazione, inclusi agenzie governative, singoli funzionari governativi, qualsiasi "Pubblico Funzionario" o membro dell'Assemblea Legislativa, società private e dipendenti di tali società private in qualsiasi circostanza.

Tutto il personale deve essere consapevole di qualsiasi pagamento o transazione insolita che può essere vista come una tangente, influenza sull'acquisto, frode elettorale, violazione della fiducia o denaro in cambio di onorificenze. Qualsiasi incertezza o domanda deve essere riferita all'MLRO. Se il personale sospetta un'attività di corruzione, è necessario presentare all'MLRO un modulo di segnalazione interna di attività sospette.