Società San Lidano Cooperativa

Regole Comportamentali Ex D.lgs. 231/2001

Reati Presupposto Articolo 24bis D.lgs 231/2001

1. INTRODUZIONE

Il presente documento costituisce protocollo comportamentale del sistema ex D.lgs. 231/2001, adottato da **SAN LIDANO COOPERATIVA** ai fini della prevenzione e mitigazione del rischio potenziale per la commissione dei Reati Presupposto di cui al Catalogo ex D.lgs. 231/2001.

Costituisce, quini, parte integrante del Modello di Organizzazione adottato da **SAN LIDANO COOPERATIVA**, quale norma comportamentale inderogabile.

La violazione – commissiva e/o omissiva – delle regole di cui al presente documento costituisce fatto disciplinarmente rilevante con legittima adozione dei provvedimenti disciplinari di cui al C.c.n.l. di riferimento, applicato da **SAN LIDANO COOPERATIVA**.

I principi generali di controllo posti a base degli strumenti e delle metodologie utilizzate per strutturare i presidi specifici di controllo sono così individuati e sintetizzati:

esistenza di protocolli: esistenza di disposizioni aziendali idonee a fornire principi di comportamento, ruoli e responsabilità, modalità operative e controlli per lo svolgimento delle attività sensibili, nonché modalità di archiviazione della documentazione rilevante;

tracciabilità e verificabilità ex post delle attività/operazioni/ transazioni tramite adeguati supporti documentali/informatici: per ogni operazione vi deve essere un adeguato supporto documentale su cui si possa procedere in ogni momento alla effettuazione di controlli che attestino le caratteristiche e le motivazioni della operazione ed individuino chi abbia autorizzato, effettuato, registrato e verificata l'operazione stessa. La salvaguardia di dati e procedure in ambito informatico può essere assicurata mediante l'adozione delle misure di sicurezza già prevedute dal D.lgs. 196/2003 e ss. mm. e ii. per tutti i trattamenti di dati effettuati con strumenti elettronici;

segregazione dei compiti: il sistema deve garantire l'applicazione dei principi di separazione di funzioni, per cui l'autorizzazione alla effettuazione di una operazione deve avere luogo sotto la responsabilità di soggetti diversi da quello che esegua operativamente o controlli l'operazione. Inoltre: a) i poteri e le responsabilità debbono essere chiaramente definiti e conosciuti all'interno della organizzazione; b) i poteri autorizzativi e di firma debbono essere coerenti con le responsabilità organizzative assegnate; c) adeguata conoscenza all'interno della organizzazione aziendale e della struttura, dei poteri autorizzativi e di firma. Ogni atto attributivo di funzioni deve rispettare gli specifici requisiti eventualmente richiesti dalla legge. La segregazione è garantita, all'interno di uno stesso macro processo aziendale, da più soggetti al fine di garantire indipendenza ed obiettività dei processi, anche facendo ricorso a sistemi informatici che abilitino talune operazioni solo a persone identificate ed autorizzate.

2. ARTICOLO 24BIS - FATTISPECIE REATI PRESUPPOSTO

Il presente documento costituisce regola comportamentale inderogabile in relazione alle fattispecie di Reato Presupposto ex articolo 24bis D.lgs. 231/2001 – Delitti informatici e trattamento illecito di dati – Articolo aggiunto dalla Legge nr. 48/2008, modificato dal D.lgs. nn. 7 e 8/2016 e dal L.L. nr. 105/2019, modificato dalla Legge nr. 90/2024:

Documenti informatici (art. 491-bis c.p.)

Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.) [articolo modificato dalla Legge n. 90/2024]

Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615-quater c.p.) [articolo modificato dalla Legge n. 238/2021 e modificato dalla Legge n. 90/2024]

Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.) [articolo modificato dalla Legge n. 238/2021 e dalla Legge n. 90/2024]

Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.) [articolo modificato dalla Legge n. 238/2021 e dalla Legge n. 90/2024]

Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.) [articolo modificato dalla Legge n. 90/2024]

Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter c.p.) [articolo modificato dalla Legge n. 90/2024]

Danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.) [articolo modificato dalla Legge n. 90/2024]

Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 635-quater.1 c.p.) [articolo introdotto dalla Legge n. 90/2024]

Danneggiamento di sistemi informatici o telematici di pubblico interesse (art. 635-quinquies c.p.) [articolo modificato dalla Legge n. 90/2024]

Frode informatica del certificatore di firma elettronica (art. 640-quinquies c.p.)

Violazione delle norme in materia di Perimetro di sicurezza nazionale cibernetica (art. 1, comma 11, D.L. 21 settembre 2019, n. 105)

Estorsione (art. 629, comma 3, c.p.) [articolo aggiunto dalla Legge n. 90/2024]

3. ILLUSTRAZIONE FATTISPECIE REATI EX ARTICOLO 24BIS

Documenti informatici (articolo 491 bis c.p.)

Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private.

Accesso abusivo ad un sistema informatico o telematico (articolo 615 ter c.p.)

Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni. La pena è della reclusione da uno a cinque anni: 1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema; 2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato; 3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti. Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni (Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.

Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (articolo 615 quater c.p.)

Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente riproduce, si procura, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a 5164 euro. La pena è della reclusione da uno a due anni e della multa da 5163 euro a 10329 euro se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'art. 617 quater.

Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (articolo 615 quinquies c.p.)

Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, e` punito con la reclusione fino a due anni e con la multa sino a euro 10.329.

Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (articolo 617 quater c.p.)

Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni. Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma. I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa. Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso: 1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità; 2) da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema; 3) da chi esercita anche abusivamente la professione di investigatore privato.

Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (articolo 617 quinquies c.p).

Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni. La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617-quater.

Danneggiamento di informazioni, dati e programmi informatici (articolo 635 bis c.p.)

Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni e si procede d'ufficio.

Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (articolo 635 ter c.p.)

Salvo che il atto costituisca piu` grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni. Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena e` della reclusione da tre a otto anni. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto e` commesso con abuso della qualità di operatore del sistema, la pena e` aumentata.

Danneggiamento di sistemi informatici o telematici (articolo 635 quater c.p)

Salvo che il fatto costituisca piu` grave reato, chiunque, mediante le condotte di cui all'articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento e` punito con la reclusione da uno a cinque anni. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

Danneggiamento di sistemi informatici o telematici di pubblica utilità (articolo 635 quinquies c.p.)

Se il fatto di cui all'articolo 635- quater e` diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilita` o ad ostacolarne gravemente il funzionamento, la pena e` della reclusione da uno a quattro anni. Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilita` ovvero se questo e` reso, in tutto o in parte, inservibile, la pena e` della reclusione da tre a otto anni. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto e` commesso con abuso della qualità di operatore del sistema, la pena e` aumentata.

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

Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti alla legge per il rilascio di un certificato qualificato, e` punito con la reclusione fino a tre anni e con la multa da 51 a 1.032 euro

Violazione delle norme in materia di Perimetro di sicurezza nazionale cibernetica (articolo 1, comma 11, D.L. 21 settembre 2019, n. 105)

Chiunque allo scopo di ostacolare o condizionare:

l'espletamento dei procedimenti di compilazione e aggiornamento degli elenchi delle reti, dei sistemi informativi e dei servizi informatici e dei procedimenti relativi all'affidamento di forniture di beni, sistemi e servizi ICT destinati a essere impiegati sulle reti, sui sistemi informativi o le attività ispettive e di vigilanza da parte della Presidenza del Consiglio dei ministri e del Ministero dello sviluppo economico, forniscono informazioni, dati o fatti non rispondenti al vero rilevanti per l'aggiornamento degli elenchi su ricordati o ai fini delle comunicazioni previste nei casi di affidamento di forniture di beni, sistemi e servizi ICT destinati ad essere impiegati sulle reti, o per lo svolgimento delle attività ispettive e di vigilanza; oppure omettono di comunicare i predetti dati, informazioni o elementi di fatto, rispondono dell'illecito con la pena della reclusione da uno a tre anni.

4. PRINCIPALI AREE AZIENDALI RISULTANTI A RISCHIO

4.1. Il rischio inerente è il rischio di un evento senza considerare i controlli o le misure di mitigazione implementate per gestirlo. Il rischio residuo, invece, è il rischio che rimane dopo che sono stati implementati i controlli e le misure di mitigazione. In sostanza, il rischio inerente è il rischio "lordo" o "potenziale", mentre il rischio residuo è il rischio "netto" o "effettivo".

Rischio Inerente:

È il livello di rischio intrinseco a un'attività o processo senza considerare le misure di controllo o le azioni intraprese per gestirlo. Si tratta del rischio "potenziale" o "lordo", che riflette la probabilità di un evento negativo e il suo potenziale impatto.

Rischio Residuo:

È il livello di rischio rimanente dopo aver implementato i controlli e le misure di mitigazione. Riflette il livello di rischio "effettivo" o "netto", tenendo conto delle azioni intraprese per gestire i rischi inerenti.

Relazione tra Rischio Inerente e Residuo:

Il rischio residuo è sempre inferiore al rischio inerente, poiché le misure di mitigazione sono progettate per ridurre il rischio. La differenza tra i due valori è un indicatore dell'efficacia dei controlli implementati.

Importanza della Gestione del Rischio:
La gestione del rischio, che include l'analisi dei rischi inerenti e la valutazione dei rischi residui, è un processo continuo che mira a ridurre i rischi e a proteggere gli interessi di un'organizzazione.

4.2. Con riferimento alla fattispecie di Reato presupposto ex articolo 24bis D.lgs. 231/2001, le funzioni aziendali coinvolte e le principali attività sensibili imputabili risultanti sono:

- CdA;
- Direzione Generale;
- Aree Personale e Commerciale;
- Area Sistema IT;
- Responsabili Procedimenti Aree riferimento

In relazione all'attività svolta dalla **SAN LIDANO COOPERATIVA**, dalla Mappatura delle concrete potenzialità commissive dei reati in oggetto è risultato quanto segue:

- una valutazione generale di bassa gravità associata ai processi aziendali che possono costituire rischio di reato;
- una valutazione specifica di media gravità.

Costituiscono situazioni di attenzione nell'ambito delle suddette funzioni le attività associate al potenziale danneggiamento di informazioni, dati e programmi telematici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità.

Costituiscono situazione di attenzione nell'ambito delle funzioni ed aree di attività i seguenti macro-processi / processi:

- richieste e utilizzo di contributi, sovvenzioni, finanziamenti nazionali o comunitari;
- gestione delle ispezioni da parte di Enti della Pubblica Amministrazione;
- rapporti con P.A. per ottenimento di licenze, autorizzazioni, concessioni;
- gestione dei rapporti con Organi istituzionali anche solo potenzialmente coinvolti nei processi inerenti l'esecuzione dell'attività di **SAN LIDANO COOPERATIVA**;
- rapporti di qualsiasi natura con soggetti ed istituzioni private;
- offerte, richiesta e gestione dell'acquisto di prodotti e servizi funzionali alla esecuzione dell'attività;
- assunzione e gestione del personale; gestione rimborsi spese e carte di credito.

Altre fattispecie sono rilevate in ottica di mera potenzialità astratta.

5. REGOLE GENERALI

5.1. Tutti i Destinatari del Modello di Organizzazione, come individuati nella Parte Generale, adottano regole di condotta conformi ai principi contenuti nel Codice Etico di **SAN LIDANO COOPERATIVA**, al fine di prevenire il verificarsi dei Reati presupposto ex articolo 24bis D.lgs. 231/2001.

Tutte le Attività Sensibili devono essere svolte conformandosi alle leggi vigenti, alle disposizioni del Modello di Organizzazione, del Codice Etico, dello Statuto, nonché alle regole e prescrizioni comportamentali contenute nel presente Regolamento.

Al CdA, alla Direzione Generale, ai Responsabili ed Addetti alle funzioni operative, ai Dipendenti, ad ogni Collaboratore e/o Consulente, al Collegio Sindacale è fatto divieto di porre in essere - da soli o in concorso con soggetti terzi - comportamenti che integrino le fattispecie di reato previste nell'articolo 25bis

5.2. SAN LIDANO COOPERATIVA deve essere dotata di strumenti organizzativi, informatici e gestionali improntati ai principi generali di:

- conoscibilità degli stessi all'interno di **SAN LIDANO COOPERATIVA**;
- tracciabilità dei flussi;
- messa in sicurezza dei dati e delle informazioni sensibili e riservate;
- chiara e formale delimitazione dei ruoli, con una completa descrizione dei compiti di ciascuna funzione e dei relativi poteri e responsabilità;
- chiara descrizione delle linee di riporto;
- adeguato livello di formalizzazione, per rendere possibile la tracciabilità delle attività svolte da chi opera per conto della stessa;
- svolgimento dell'attività conformemente alle prescrizioni del " *Processo di Procedimento* " adottato da **SAN LIDANO COOPERATIVA**;
- modalità e periodicità di cambiamento della password;
- destituzione dei diritti di accesso in caso di cessazione e/o cambiamento del tipo di rapporto che attribuiva il diritto di accesso ed utilizzo del sistema informatico e contestuale immediato cambio dei relativi codici di accesso.

Al CdA, al Direttore Generale, ai Responsabili ed Addetti alle funzioni operative, ai Dipendenti, ad ogni Collaboratore e/o Consulente, al Collegio Sindacale è fatto divieto di porre in essere - da soli o in concorso con soggetti terzi - comportamenti che integrino le fattispecie di reato previste nell'articolo 24bis D.lgs. 231/2001.

6. REGOLE/OBBLIGHI COMPORTAMENTALI

6.1. I seguenti obblighi di carattere generale si applicano al CdA, alla Direzione Generale, ai Responsabili ed Addetti alle funzioni operative nonché a soggetti terzi a **SAN LIDANO COOPERATIVA**, che operino anche in forza di rapporti consulenziali e/o di collaborazione.

E' fatto espresso obbligo a carico dei soggetti sopra indicati di:

- tenere un comportamento corretto e trasparente, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività in cui è coinvolta la P.A. ed ogni altro soggetto terzo;
- assicurare il corretto svolgimento di tutti i processi in cui ci si interfaccia con la P.A. ed ogni altro soggetto terzo;
- conformarsi alle procedure ed alle prescrizioni di tutela e sicurezza del sistema informatico e della riservatezza dei dati sensibili come di ogni altra informazione acquisita e/o gestita nella esecuzione del servizio affidato, nei confronti della P.A., come di ogni altro soggetto terzo, interno come esterno, funzionale alla organizzazione ed alla esecuzione/svolgimento dell'attività e dei rapporti negoziali intrattenuti;

- impegnarsi a non rendere pubbliche tutte le informazioni assegnate e/o gestite per l'utilizzo delle risorse informatiche e l'accesso a dati e sistemi (avuto particolare riguardo allo username ed alla password);
- attivare ogni misura ritenuta necessaria per la protezione del sistema e dei dati, evitando che terzi possano avere accesso allo stesso in caso di allontanamento dalla postazione;
- accedere ai sistemi informativi unicamente attraverso i codici identificativi assegnati a ciascun soggetto e procedere alla modifica periodica della password entro le scadenze indicate;
- non intraprendere azioni atte a superare le protezioni applicate ai sistemi informativi aziendali;
- non installare alcun programma, anche se attinente all'attività aziendale, senza aver prima interpellato il Responsabile per la Sicurezza Informatica e la Direzione Generale;
- non accedere, senza specifica autorizzazione, a sistemi informativi di terzi, né alterarne in alcun modo il funzionamento, al fine di ottenere e/o modificare, senza diritto, dati, programmi, informazioni;
- non connettersi, consultare, navigare, effettuare attività di streaming ed estrarre mediante downloading, a siti web che siano considerati illeciti (contro la morale pubblica, alla libertà di culto, alla violazione della Privacy, contrari all'ordine pubblico, ecc.).

6.2. E' fatto espresso divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, considerati individualmente o collettivamente, integrino gli estremi di un reato. In particolare, è fatto divieto di:

- diffondere, propalare, divulgare dati, informazioni, notizie acquisite nell'esercizio della funzione;
- violare i sistemi di sicurezza del sistema informatico;
- tenere una condotta negligente nell'ambito della gestione del sistema informatico;
- violare, anche solo a livello di tentativo, le suesposte regole.

6.3. Procedure specifiche

In un'ottica special-preventiva, devono essere altresì rispettate le seguenti regole:

- agli Esponenti aziendali che intrattengono rapporti con esponenti della P.A. e con Partners/stakeholders inerenti l'attività di servizio, per conto di **SAN LIDANO COOPERATIVA**, deve essere formalmente conferita delega, ovvero essere dotati dei poteri propri della funzione, mentre ai soggetti terzi un incarico espresso nel relativo contratto;
- di ogni criticità di rilievo, anche solo potenziale, che venga rilevata nel sistema informatico, a livello di non adeguata gestione e/o tutela dei dati, ovvero di uso distorto ed anche solo potenzialmente non lecito, ovvero di violazione e/o di intromissione, anche a livello di tentativo del sistema informativo, ovvero di rilevato deficit di sicurezza dello stesso, deve essere immediatamente e tempestivamente informato l'Amministratore di Sistema, la Direzione Generale, nonché l'Organismo di Vigilanza, affinché vengano presi i provvedimenti atti ad eliminare la problematica evidenziata;
- i soggetti terzi devono essere individuati mediante procedure trasparenti e con parità di trattamento, per prestazioni di lavoro autonomo o temporaneo, con adeguata tutela normativa e di sicurezza dei dati sensibili acquisiti;
- i contratti con i soggetti terzi devono contenere clausole standard, che impongano loro il rispetto del sistema di prevenzione dalla commissione di reati presupposto, ex D.lgs. 231/2001, ai sensi del Modello di Organizzazione e del Codice Etico adottato da **SAN LIDANO COOPERATIVA**;

- le dichiarazioni rese ad Organismi pubblici nazionali o comunitari ai fini dell'ottenimento di contributi o finanziamenti, devono avere luogo attraverso il sistema informatico, nel rispetto delle procedure di sicurezza e riservatezza, del rispetto delle procedure prevedute dagli Organismi;
- gli Esponenti aziendali esercenti funzione di controllo e supervisione su adempimenti connessi all'espletamento delle suddette attività devono porre particolare attenzione sulla corretta attuazione degli adempimenti stessi e riferire immediatamente eventuali situazioni di irregolarità o anomalie, anche solo potenziali, all'Organismo di Vigilanza;
- gestire, nell'assoluto rispetto di ogni tutela, i dati sensibili del personale dipendente, dei Collaboratori, dei Fornitori
- coloro i quali siano competenti alla redazione ed alla trasmissione per via informatica o telematica ad enti della P.A. di report, di rendiconti periodici o su richiesta, dovranno essere a ciò formalmente incaricati e dovranno operare conformandosi alle prescrizioni comportamentali ed alle cautele previste per la prevenzione dalla commissione di dei Reati Informatici, ex articolo 24 bis;
- alle ispezioni giudiziarie, tributarie e amministrative devono partecipare i soli Esponenti aziendali a ciò espressamente delegati. Del procedimento di ispezione devono essere redatti e conservati appositi verbali, prontamente comunicati all'Organismo di Vigilanza, laddove riportino contestazioni o irregolarità;
- ogni corrispondenza o reporting destinati agli Enti ed Organi della P.A. deve essere effettuata mediante trasmissione di " *posta certificata* ", con archiviazione (informatica o cartacea) della relativa documentazione.
-

6.4. Regole Comportamentali

SAN LIDANO COOPERATIVA ha adottato un insieme di regole idoneo a garantire sia la sicurezza delle reti e dei Sistemi informatici e telematici, che l'ambiente di lavoro e l'immagine di **SAN LIDANO COOPERATIVA**.

In particolare ciascun esponente aziendale:

- dovrà utilizzare (senza poterne dare comunicazioni a terzi), con le modalità indicate, lo User ID e la *password* individuale di autorizzazione all'accesso al Sistema informatico aziendale, o gli eventuali sistemi di identificazione ed autenticazione alternativi (es. utilizzo di lettori di impronte digitali e *smart card*) in modo personale, garantendo quindi la segretezza degli stessi; è vietato l'uso, dei suddetti dispositivi da parte di soggetti diversi dall'intestatario;
- dovrà utilizzare personalmente le credenziali che consentono l'accesso all'Intranet aziendale ed ai relativi servizi, senza poterle condividere o cedere a terzi;
- dovrà operare sui computer aziendali esclusivamente per lo svolgimento di attività lavorative, salve specifiche autorizzazioni rilasciate dal Responsabile Aziendale di riferimento. In particolare, è vietato l'ascolto di programmi e files video, audio o musicali, se non a fini prettamente lavorativi;
- dovrà navigare in Internet e utilizzare la posta elettronica per finalità esclusivamente legate all'espletamento delle proprie mansioni. E' tollerato l'uso personale esclusivamente se occasionale e motivato e sempre che non abbia effetti negativi in ordine al livello della performance dei Sistemi o dell'attività lavorativa generale, né alcun impatto, anche solo potenziale, sullo standard di sicurezza del sistema;
- non dovrà visitare siti Internet, nè inviare e-mail contenenti materiale illegale (ad esempio, materiale pedopornografico), nè scaricare, senza espressa autorizzazione da parte delle strutture competenti, software gratuiti (*freeware* e *shareware*) prelevati da siti Internet (tutti i files di provenienza incerta o

esterna, ancorché attinenti all'attività lavorativa, devono essere sottoposti al controllo antivirus), nè caricare, scaricare o trasmettere in qualsiasi modo *software* o altro materiale in violazione alle leggi sul *copyright* o dei diritti riservati del legittimo proprietario;

- prima di utilizzare una fonte, un'informazione, testi o immagini, all'interno dei propri lavori, dovrà richiedere l'autorizzazione della fonte, citandola esplicitamente nel proprio documento, come previsto dalla legge sul Diritto d'Autore;
- non è consentita l'effettuazione di transazioni finanziarie, ivi comprese le operazioni di *remote banking*, acquisti online e simili, se non ai soggetti formalmente incaricati dalla Direzione Generale e nel rispetto delle normali procedure di acquisto;
- dovrà controllare i file allegati alla posta elettronica prima del loro utilizzo e non eseguire *download* di file eseguibili; ove sia dubbia l'attendibilità del mittente è vietato aprire i messaggi senza aver contattato il Responsabile dei Sistemi Informatici aziendale;
- non dovrà sollecitare corrispondenza elettronica senza relazioni con le attività aziendali, nè promuovere affari estranei all'oggetto dell'attività aziendale, anche a fini di lucro o di profitto personale;
- non dovrà utilizzare il servizio di posta per condurre attacchi a computer esterni alla rete, o inficiare la corretta operatività di sistemi altrui, o per diffondere software " *illegale* " (virus, ecc.);
- non dovrà utilizzare, nè installare *software* atti ad intercettare, falsificare, alterare il contenuto di documenti informatici;
- sono vietati comportamenti atti al danneggiamento di informazioni, dati e/o programmi dei Sistemi informativi di pubblica utilità e/o dello Stato e/o di altro Ente Pubblico ai quali, per motivi di lavoro, si possiedano le autorizzazioni per accedere;
- non dovrà modificare la configurazione hardware e software della postazione di lavoro (fissa e/o mobile), aggiungendo o rimuovendo componenti, modificando lo standard aziendale, al fine di non danneggiare e/o interrompere il sistema informativo o telematico dell'azienda;
- garantire il back-up di informazioni e software;
- proteggere la sicurezza del sistema informatico e dei dati;
- consentire l'identificazione dell'utilizzo del sistema e/o del programma aziendale;
- consentire la tracciabilità e la ricostruzione ex post dell'utilizzo e dell'utilizzatore del sistema informatico e/o del programma aziendale;
- la custodia dei dispositivi di memorizzazione (esempio, chiavi USB, CD, hard disk ecc.);
- garantire la confidenzialità, autenticità ed integrità delle informazioni.

7. FUNZIONI PECULIARI DELL'ODV SU TALI RISCHI - REATO

Tra le funzioni peculiari dell'Organismo di Vigilanza nell'ambito della fattispecie di Reati presupposto ex articolo 24bis, ferma restando la facoltà di auto- organizzazione dell'Organismo, si evidenziano:

- monitoraggio sistema IT, per la verifica delle procedure e del rispetto dei principi comportamentali esposti, ai fini della sicurezza del sistema;

- esame di eventuali segnalazioni specifiche, anche rese in via anonima ed assunzione delle iniziative necessarie od opportune;
- verifica specifica, in caso di modifica dell'assetto organizzativo e del Sistema delle deleghe di poteri vigenti, delle procedure e del rispetto dei principi comportamentali esposti;
- coordinamento e flusso informativo con il Responsabile del Sistema Informativo nella definizione delle procedure della gestione e della sicurezza del sistema informatico.

Il CdA, la Direzione Generale e i Responsabili e gli Addetti delle Aree aziendali interessate, nell'ambito delle proprie competenze e funzioni, devono inviare all'OdV - con assoluta ed inderogabile tempestività - ove ricorra un fatto di rilievo, ogni dato, informazione, documentazione aggiornamento, avente rilevanza fattuale o di natura giuridica, attinente, strumentale od oggetto dell'azione prevenzionistica della commissione dei Reati presupposto ex articolo 24bis D.lgs. 231/2001.

I risultati dell'attività di vigilanza e controllo nell'ambito dell'articolo 24bis D.lgs. 231/2001 sono comunicati dall'OdV all'Organo di governo nelle Relazioni periodiche, ovvero tempestivamente allorquando ricorrano particolari esigenze o a discrezione dell'OdV stesso.

8. SANZIONI DISCIPLINARI

8.I. I principi, le procedure e gli obblighi contenuti nel Modello adottato da **SAN LIDANO COOPERATIVA** costituiscono obbligazioni contrattuali del prestatore di lavoro, ai sensi e per gli effetti dell'articolo 2104 cod. civ. giusta la prescrizione dell'articolo 7, comma quarto, lett. b), D.lgs. 231/2001.

Il Sistema Disciplinare Interno costituisce il complesso organico di prescrizioni regolanti le procedure interne di rilevazione, accertamento, contestazione della violazione del Modello (comprensivo del Codice etico e delle regole di condotta prescritte dai Protocolli), nonché di successivo sanzionamento del trasgressore.

Esso è conformato alle norme di cui allo Statuto dei Lavoratori, legge 20 maggio 1970, n. 300, con riguardo ai diritti ed alle garanzie del Lavoratore, nonché alle prescrizioni di cui al CCNL applicato da **SAN LIDANO COOPERATIVA**. L'obbligazione espressa di rispettare tali disposizioni viene altresì ribadita nei contratti di collaborazione, di qualsiasi tipo, stipulati dalla Società con i Terzi.

Per ogni trasgressione troveranno applicazione sanzioni disciplinari proporzionate e adeguate, nel rispetto dell'articolo 2106 cod. civ. alla gravità delle mancanze e comunque valutate in base ai seguenti criteri:

- elemento soggettivo della condotta (intenzionalità del comportamento o grado di negligenza);
- rilevanza degli obblighi violati;
- collocazione gerarchica/funzionale dell'autore della violazione;
- conseguenze e potenzialità di danno per **SAN LIDANO COOPERATIVA**;
- ricorrenza di eventuali circostanze aggravanti/attenuanti;
- eventuale concorso di più soggetti;
- recidiva.

La violazione commessa configura un illecito disciplinare a prescindere dall'eventuale instaurazione di azioni giudiziarie in sede penale, civile o strettamente contrattuale.

In particolare, per le violazioni delle prescrizioni del Modello penal-preventivo adottato da **SAN LIDANO COOPERATIVA** trovano applicazione le seguenti misure sanzionatorie:

- per i Dirigenti, misure nel rispetto del Contratto Collettivo Nazionale di Lavoro applicabile ("CCNL Dirigenti");
- per i Lavoratori dipendenti - che non abbiano la qualifica di dirigenti - sanzioni disciplinari ai sensi dell'art. 2106 cod. civ. e dell'art. 7 dello Statuto dei Lavoratori, L. 300/1970, nel rispetto delle prescrizioni del Contratto Collettivo Nazionale di Lavoro di riferimento;
- clausole contrattuali di natura sanzionatoria e/o risolutoria, salvo la richiesta di risarcimento danni, inserite nei contratti stipulati con Collaboratori, Intermediari,
- misure alternative che inducano al rispetto delle suddette disposizioni, nei confronti di coloro verso i quali non è possibile applicare le misure sopra previste.

L'OdV controllerà che le misure sopra elencate siano applicate regolarmente ed efficacemente.

Nel caso in cui con una sola azione od omissione vengano commesse più infrazioni, ciascuna delle quali punita con una sanzione specifica, verrà irrogata la sanzione più grave.

8.II. Infrazioni Membri Organi Sociali

SAN LIDANO COOPERATIVA valuta con rigore le infrazioni alle prescrizioni del Modello vigente poste in essere dai Vertici aziendali (Organo amministrativo ed Organi di controllo), tenuti a rappresentare l'immagine di **SAN LIDANO COOPERATIVA** presso Dipendenti, Soci e S*takeholders*.

La formazione ed il consolidamento di un'etica aziendale sensibile ai valori della correttezza, della trasparenza e della legalità presuppone, anzitutto, che tali valori siano acquisiti e rispettati da chi esercita la *leadership* aziendale, in modo da costituire esempio e stimolo nei confronti di chi opera con/per la Società.

All'OdV è riconosciuto il potere di interloquire con gli Organi societari e la facoltà di sollecitare la verifica della sussistenza degli elementi richiesti per legge ai fini dell'esercizio delle azioni di responsabilità e/o di revoca per " *giusta causa* ". In caso di violazione delle procedure interne previste dal Modello da parte dei membri degli organi di gestione e/o di controllo, l'OdV in ragione del fatto che la violazione sia stata commessa da un singolo membro, ovvero dall'intero organo collegiale, informerà tempestivamente l'Organo di amministrazione e/o il Collegio Sindacale e/o l'Assemblea, per la pronta assunzione delle opportune iniziative e i conseguenti provvedimenti.

Anche nell'interesse del membro dell'Organo autore della violazione, l'OdV proporrà all'Organo amministrativo, al Collegio Sindacale e/o, se del caso all'Assemblea, i provvedimenti idonei alla eventuale sospensione temporanea dall'esercizio dei poteri/ funzioni ad esso attribuiti, per il tempo necessario all'effettuazione degli accertamenti di responsabilità.

8.III. Infrazioni dei Dirigenti.

In caso di violazione del Dirigente (i.e. direttori, condirettori, vice-direttore, institori, procuratori con stabile mandato *ad negotia*), si provvederà ad applicare le misure ritenute più idonee in conformità a quanto previsto dal CCNL Dirigenti applicato.

In particolare:

1. Trasgressioni che non comportano la risoluzione del rapporto di lavoro

Le violazioni da parte del Dirigente, salvo che non comportino la risoluzione del rapporto

di lavoro nei casi indicati nel presente Sistema Disciplinare, devono essere annotate nel suo stato di servizio.

L'annotazione è strumentale anche al rilevamento di eventuali recidive.

Tali infrazioni saranno considerate dall'Organo amministrativo in sede di determinazione degli emolumenti, fatti salvi gli scatti di anzianità previsti dal CCNL Dirigenti.

2. Trasgressioni che comportano la risoluzione del rapporto di lavoro

La violazione che per gli altri lavoratori subordinati comporterebbero la sanzione del licenziamento, daranno luogo alla risoluzione del rapporto di lavoro del Dirigente nei modi previsti dal CCNL Dirigenti (licenziamento con contestuale motivazione).

4. Infrazioni dei Quadri e dei Lavoratori Subordinati.

Il Modello è portato a conoscenza di tutti i Dipendenti di **SAN LIDANO COOPERATIVA** con qualsiasi modalità (affissione in bacheca, consegna di copia dello stesso, intranet aziendale) nonché attraverso la tenuta di specifici corsi informativi e formativi.

I comportamenti tenuti dai Dipendenti in violazione delle singole regole comportamentali costituiscono inadempimento alle obbligazioni primarie del rapporto di lavoro e configurano illeciti di natura disciplinare.

Le sanzioni rientrano tra quelle previste dalla normativa vigente e dal Capitolo DISCIPLINA del vigente Contratto Collettivo Nazionale di riferimento.

In particolare, l'inosservanza dei doveri e delle prescrizioni comporta, a seconda dell'entità della violazione valutata in base alle prescrizioni del CCNL**,** l'applicazione dei seguenti provvedimenti sanzionatori:

1) Incorre nei provvedimenti di Rimprovero scritto il lavoratore che:

violi le procedure interne previste dal presente Modello (ad es. che non osservi le procedure prescritte, ometta di dare comunicazione all'Organismo di Vigilanza delle informazioni prescritte, ometta di svolgere controlli, ecc.) o adotti, nell'espletamento di Attività sensibili, un comportamento non conforme alle prescrizioni del Modello stesso.

2) Incorre, inoltre, anche nel provvedimento di Multa di importo variabile fino al massimo di 4 ore di retribuzione, ovvero nel provvedimento di Sospensione dal lavoro e dalla retribuzione fino ad un massimo di 10 giorni, il lavoratore che:

adotti nell'espletamento delle Attività sensibili un comportamento non conforme alle prescrizioni del Modello e diretto in modo univoco al compimento di un reato sanzionato dal D.lgs. 231/2001 e successive modifiche e integrazioni.

3) Può incorrere, infine, anche nel provvedimento di licenziamento il lavoratore che adotti, nell'espletamento delle Attività sensibili un comportamento palesemente in violazione delle prescrizioni del Modello, tale da determinare la concreta applicazione a carico della Società di misure previste dal Decreto.

Le sanzioni di cui ai punti 2 e 3 saranno commisurate alla gravità dell'infrazione e alla reiterazione della stessa (della recidività si terrà conto anche ai fini della comminazione di una eventuale sanzione espulsiva).

Per quanto riguarda l'accertamento delle suddette infrazioni, procedimenti disciplinari e l'irrogazione delle sanzioni, restano invariati i poteri già conferiti, nei limiti della rispettiva competenza, al Management aziendale.

Il Sistema Disciplinare viene costantemente monitorato dalla Funzione Personale con la supervisione dell'Organismo di Vigilanza.

8.IV. Infrazioni dei Collaboratori Esterni e dei Partners

Le violazioni del Modello per quanto questo risulti applicabile a Terzi, Fornitori di beni e/o di servizi e Collaboratori esterni - fatta salva l'azione di risarcimento di eventuali danni sofferti da **SAN LIDANO COOPERATIVA** - comporterà l'applicazione immediata delle misure previste quali clausole contrattuali di "*risoluzione ipso iure*", negli atti di conferimento dell'incarico.

Le violazioni danno luogo alla risoluzione del rapporto contrattuale per inadempimento imputabile ex articolo 1453 cod. civ. ovvero comportano la risoluzione immediata e di diritto del rapporto nei modi previsti dall'articolo 1456 cod. civ. A tal fine viene preveduta una "*clausola risolutiva espressa*" nel contratto di conferimento d'incarico, ovvero nel documento che sostanzia l'instaurazione di un rapporto continuativo tra **SAN LIDANO COOPERATIVA** ed il Collaboratore esterno, anche mediante un *addendum* al contratto da tempo stipulato che ne risulti privo. **SAN LIDANO COOPERATIVA** potrà sottoporre a tali soggetti, anche successivamente all'instaurazione del rapporto, un modulo di dichiarazione di conoscenza e presa d'atto della vigenza del Codice Etico, nonché dei Protocolli limitatamente alla sezione regolante il funzionamento del Servizio aziendale/ funzione con la quale lo stesso entra in relazione, il quale dovrà datare e sottoscrivere per incondizionata accettazione.

9. PRINCIPI PROCEDURALI

L'OdV, nell'esercizio delle proprie funzioni di vigilanza del Modello, è chiamato a rilevare eventuali violazioni, accertandole direttamente nel corso di verifiche, ispezioni, controlli, ovvero indirettamente, a fronte di segnalazioni e comunicazioni inviate dal Responsabile del Servizio aziendale interessato, o dal responsabile della Funzione Personale, ovvero dal singolo Collaboratore, anche in forma anonima.

SAN LIDANO COOPERATIVA ha adottato un Regolamento della procedura di segnalazione.

Tale segnalazione potrà essere effettuata con qualsiasi strumento di comunicazione idoneo a garantirne l'anonimato e la riservatezza e non potrà mai giustificare azioni di ripercussione sull'autore della segnalazione, ancorché sia stata accertata l'infondatezza di essa.

Ove sia rilevata una possibile violazione, l'OdV espleterà un'attività istruttoria volta all'accertamento della violazione e della sua gravità, nel rispetto delle prescrizioni e dei principi di tutela del Lavoratore sanciti nello Statuto dei Lavoratori, nonché delle procedure all'uopo previste dal CCNL applicato.

All'esito ne verrà data comunicazione formale all'Organo dirigente di **SAN LIDANO COOPERATIVA** che, quale Datore di lavoro, attiverà la procedura disciplinare, fatto salvo l'eventuale ricorso al Giudice del Lavoro e/o di eventuali Organi conciliatori, se attivabili.

Sebbene resti in capo al Datore di lavoro l'irrogazione della sanzione disciplinare, l'OdV potrà fornire parere consultivo (non obbligatorio, né vincolante) circa la congruità della sanzione individuata e la sua concreta attitudine ad eliminare la reiterazione della violazione, come ulteriori violazioni della medesima specie.

Sezze, li 23 luglio 2025

L'OdV

Avvocato Giuseppe Ibello