

## **Procedura per la gestione delle segnalazioni interne ex D. Lgs. n. 24/2023 (c.d. Whistleblowing)**

### **Responsabilità**

	<b>Nome</b>	<b>Funzione</b>
<b>Elaborato da:</b>	Martina Dell'Elce	Organizzazione, Risorse Umane e Sistemi Corporate
<b>Verificato da:</b>	Paolo Tortorelli	SGA
<b>Verificato da:</b>	Bruno Bertucci	Responsabile Affari legali e societari
<b>Verificato da:</b>	Andrea Roversi	DPO
<b>Verificato da:</b>	Marco Ornito	Direttore Organizzazione, Risorse Umane e Sistemi Corporate
<b>Approvato da:</b>	Consiglio di Amministrazione	Organo amministrativo

### **Lista di distribuzione**

*Pubblico*

### **Sommario modifiche**

<b>Versione</b>	<b>Data</b>	<b>Descrizione</b>
00	14/12/2023	Emissione iniziale
01	15/12/2023	Emissione finale
02	15/12/2023	Versione approvata dal C.d.A.

**Indice**

<b>1. SCOPO</b>	<b>4</b>
<b>2. CAMPO DI APPLICAZIONE</b>	<b>4</b>
<b>3. TERMINI E ABBREVIAZIONI</b>	<b>5</b>
<b>4. GENERALITÀ</b>	<b>5</b>
<b>5. MODALITÀ DI SEGNALAZIONE</b>	<b>6</b>
<b>6. CONTENUTO DELLA SEGNALAZIONE</b>	<b>6</b>
<b>7. GESTIONE DELLA SEGNALAZIONE</b>	<b>7</b>
7.1 Verifica preliminare	7
7.2 Accertamento	8
7.3 Conservazione della documentazione inerente alle segnalazioni	8
<b>8. TUTELA DELLA RISERVATEZZA</b>	<b>8</b>
<b>9. QUADRO NORMATIVO, MINIMIZZAZIONE DEL TRATTAMENTO, PROTEZIONE BY DESIGN E BY DEFAULT</b>	<b>9</b>
<b>10. ALTRE FORME DI SEGNALAZIONE</b>	<b>9</b>
<b>11. MISURE DI PROTEZIONE PER SEGN</b>	<b>10</b>
<b>12. SANZIONI</b>	<b>10</b>
12.1 Le sanzioni dell'ANAC ai sensi della norma	10
12.2 Le sanzioni di SECURE NETWORK	11
12.3 Provvedimenti per i/le lavoratori/lavoratrici dipendenti di SECURE NETWORK	12
12.4 Misure nei confronti degli amministratori e dei soggetti apicali di SECURE NETWORK	12
12.5 Misure nei confronti dei membri del collegio sindacale di SECURE NETWORK	13
12.6 Misure nei confronti di collaboratori/trici esterni di SECURE NETWORK	13

**13. RINVIO**

**13**

## 1. SCOPO

Il presente documento (di seguito, **Procedura**), adottato ai sensi del D. Lgs. n. 24/2023 (di seguito, **Norma**) in attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali (di seguito, **Direttiva Whistleblowing**), ha l'obiettivo di illustrare la procedura di gestione delle segnalazioni interne in forma anonima o confidenziale effettuate per iscritto od oralmente da parte del personale di SECURE NETWORK S.r.l. (di seguito, **SECURE NETWORK**), nonché dai/dalle suoi/sue lavoratori/lavoratrici autonomi/autonome, collaboratori/collaboratrici, somministrati/e, liberi professionisti, consulenti, volontari e tirocinanti, retribuiti e non retribuiti, gli/le azionisti/azioniste e le persone con funzione di amministrazione, direzione, controllo, vigilanza o rappresentanza, anche qualora tali funzioni siano esercitate in via di mero fatto, in relazione a comportamenti, atti od omissioni, di cui siano venuti a conoscenza nell'ambito del proprio contesto lavorativo, che ledono l'interesse pubblico o l'integrità di SECURE NETWORK e che consistono in:

- 1) illeciti amministrativi, contabili, civili o penali;
- 2) condotte illecite rilevanti ai sensi del D. Lgs. n. 231/2001 e s.m.i. (c.d. "reati presupposto") o violazioni del Modello di Organizzazione, Gestione e Controllo e del Codice Etico adottati da SECURE NETWORK ai sensi della predetta norma;
- 3) illeciti che rientrano nell'ambito di applicazione degli atti dell'UE o nazionali indicati nell'allegato alla Norma ovvero degli atti nazionali che costituiscono attuazione degli atti dell'UE indicati nell'allegato alla direttiva (UE) 2019/1937, seppur non indicati nell'allegato alla Norma, relativi ai seguenti settori: appalti pubblici; servizi, prodotti e mercati finanziari e prevenzione del riciclaggio e del finanziamento del terrorismo; sicurezza e conformità dei prodotti; sicurezza dei trasporti; tutela dell'ambiente; radioprotezione e sicurezza nucleare; sicurezza degli alimenti e dei mangimi e salute e benessere degli animali; salute pubblica; protezione dei consumatori; tutela della vita privata e protezione dei dati personali e sicurezza delle reti e dei sistemi informativi;
- 4) atti od omissioni che ledono gli interessi finanziari dell'UE;
- 5) atti od omissioni riguardanti il mercato interno, comprese le violazioni delle norme dell'UE in materia di concorrenza e di aiuti di Stato, nonché le violazioni riguardanti il mercato interno connesse ad atti che violano le norme in materia di imposta sulle società o i meccanismi il cui fine è ottenere un vantaggio fiscale che vanifica l'oggetto o la finalità della normativa applicabile in materia di imposta sulle società;
- 6) atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni di cui agli atti dell'UE nei settori indicati nei punti 3), 4) e 5) che precedono.

## 2. CAMPO DI APPLICAZIONE

La Procedura è rivolta a tutto il personale di SECURE NETWORK, ivi incluso il personale con qualifica di Dirigente, nonché ai/alle suoi/sue lavoratori/lavoratrici autonomi/autonome, collaboratori/collaboratrici, somministrati/e, liberi professionisti, consulenti, volontari e tirocinanti, retribuiti e non retribuiti, agli/alle azionisti/azioniste e alle persone con funzione di amministrazione, direzione, controllo, vigilanza o rappresentanza, anche qualora tali funzioni siano esercitate in via di mero fatto.

### 3. TERMINI E ABBREVIAZIONI

Di seguito si definiscono le abbreviazioni e i termini utilizzati all'interno della Procedura:

<b>ABBR.</b>	<b>SIGNIFICATO</b>
BU	Business Unit (Practice o Segmento di Mercato)
HR	Organizzazione, Risorse Umane e Sistemi Corporate
Resp	La/Il responsabile, le/i responsabili
Segn	Il/La Segnalante
<b>TERMINI</b>	<b>SIGNIFICATO</b>
<i>Informazioni sulle violazioni</i>	Informazioni, compresi i fondati sospetti, riguardanti violazioni commesse o che, sulla base di elementi concreti, potrebbero essere commesse nell'organizzazione presso cui la persona segnalante intrattiene un rapporto giuridico ai sensi della Norma, nonché gli elementi riguardanti condotte volte ad occultare tali violazioni.
<i>Segnalazione/i o Segnalare</i>	La comunicazione scritta od orale di Informazioni sulle violazioni.
<i>Segnalante</i>	La persona fisica che effettua la Segnalazione.
<i>Persona/e coinvolta/e</i>	La persona fisica o giuridica menzionata nella Segnalazione come persona alla quale la violazione è attribuita o come persona comunque implicata nella violazione segnalata.
<i>Ritorsione/i</i>	Qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, posto in essere in ragione della Segnalazione, della denuncia all'autorità giudiziaria o contabile o della divulgazione pubblica e che provoca o può provocare al/alla Segnalante, in via diretta o indiretta, un danno ingiusto.
<i>Violazione/i</i>	I comportamenti, atti od omissioni che ledono l'interesse pubblico o l'integrità di SECURE NETWORK e che consistono nelle condotte espressamente definite nei punti da 1) a 6) della Sezione 1 ( <i>Scopo</i> ) della Procedura.
<i>Comitato</i>	L'ufficio interno al quale è affidata la gestione del canale di segnalazione interno ai sensi della Norma.

### 4. GENERALITÀ

SECURE NETWORK, nel pieno rispetto della Direttiva Whistleblowing, della Norma e dei propri Modello di Organizzazione, Gestione e Controllo e Codice Etico adottati ai sensi del D. Lgs. n. 231/2001 e s.m.i., nonché della politica aziendale relativa alla protezione e al trattamento dei dati personali, ha attivato un canale di segnalazione interno per la gestione delle Segnalazioni.

## 5. MODALITÀ DI SEGNALAZIONE

È diritto di Segn scegliere se presentare una Segnalazione in forma anonima o meno.

Le Segnalazioni da parte di Segn possono essere inviate:

- a) in formato cartaceo (a mezzo posta ordinaria), indirizzate al Comitato, indicando per oggetto “SEGNALAZIONE” e sulla busta chiusa la dicitura “RISERVATA”; oppure
- b) tramite il canale di segnalazione interno dedicato, raggiungibile sulla piattaforma della società MYGO S.r.l. denominata “MyWhistleblowing” al seguente link: <https://areariservata.mygovernance.it/#!/WB/SECURENETWORK>. Tale canale di segnalazione interno è operativo 7 giorni su 7, 24 ore su 24, e garantisce la riservatezza dell'identità di Segn, della Persona coinvolta, di ogni persona eventualmente menzionata nella Segnalazione, nonché del contenuto della Segnalazione e della relativa documentazione in virtù del ricorso all'algoritmo di cifratura (i.e. crittografia) AES-256.

Le Segnalazioni ricevute tramite il suddetto canale di segnalazione interna sono archiviate in via riservata a cura del Comitato e conservate con tali modalità per 5 (cinque) anni, e comunque entro i termini previsti dalla normativa in vigore, a decorrere dalla data della comunicazione dell'esito finale della procedura di Segnalazione di Segn.

Tale canale di segnalazione interno consente l'effettuazione di Segnalazioni **in forma scritta e in forma orale**.

I soggetti diversi dal Comitato che dovessero ricevere una Segnalazione al di fuori del sopra citato canale di segnalazione interno devono inoltrarla tempestivamente e, comunque, **entro e non oltre 7 (sette) giorni dal suo ricevimento**, con tutta l'eventuale relativa documentazione, allo stesso Comitato, utilizzando la massima riservatezza al fine di proteggere l'identità di Segn, della Persona coinvolta, di ogni persona eventualmente menzionata nella Segnalazione, nonché il contenuto della Segnalazione e della relativa documentazione e di garantire l'efficacia della gestione della Segnalazione da parte del medesimo Comitato, anche al fine di evitare ogni forma di Ritorsione nei confronti di Segn.

## 6. CONTENUTO DELLA SEGNALAZIONE

La Segnalazione, quanto più specifica, circostanziata e dettagliata possibile, deve contenere almeno:

- a. quando la Segnalazione non è anonima, le generalità di Segn, con indicazione della mansione svolta all'interno di SECURE NETWORK;
- b. le Violazioni oggetto della Segnalazione e, se noti, il momento e il luogo in cui esse siano state commesse dalla Persona coinvolta;
- c. i concreti elementi di fatto che possano confermare l'attendibilità della Segnalazione e individuare senza equivoci la Persona coinvolta;
- d. l'indicazione di eventuali soggetti che possano confermare la Segnalazione.

Saranno considerate rilevanti unicamente Segnalazioni basate su elementi fattuali concreti inerenti le Violazioni commesse dalle Persone coinvolte nel contesto lavorativo di SECURE NETWORK.

Le Segnalazioni anonime saranno ugualmente prese in considerazione, ma dovranno essere sufficientemente dettagliate onde consentire al Comitato di dar diligente seguito alle Segnalazioni così ricevute e di dare un riscontro alle medesime.

Non saranno prese in considerazione Segnalazioni non conformi alla Norma e alla Procedura, ivi incluse quelle che riguardino contestazioni, rivendicazioni o richieste legate ad un interesse di carattere personale di Segn che attengano esclusivamente ai propri rapporti individuali di lavoro o inerenti al rapporto di lavoro con figure gerarchicamente sovraordinate al/alla medesimo/medesima Segn.

## **7. GESTIONE DELLA SEGNALAZIONE**

### **7.1 Verifica preliminare**

La gestione e la verifica preliminare sulla fondatezza delle circostanze rappresentate nella Segnalazione sono affidate **esclusivamente** al Comitato che vi provvede nel rispetto dei principi di imparzialità e riservatezza effettuando le seguenti attività:

- invia un avviso del ricevimento della Segnalazione a Segn **entro 7 (sette) giorni** a decorrere dalla data del ricevimento della Segnalazione;
- prevede un termine ragionevole per fornire un riscontro non superiore a **3 (tre) mesi a far data dall'avviso di ricevimento della Segnalazione**. Se non è stato inviato alcun avviso a Segn, il termine per il riscontro del Comitato è di **3 (tre) mesi dalla scadenza del termine di 7 (sette) giorni dalla presentazione della Segnalazione**;
- analizza la documentazione messa a disposizione da Segn e, ove ritenuto necessario, richiede a Segn eventuali integrazioni documentali o in fatto;
- intervista Segn qualora costui ne faccia richiesta, nonché eventuali altri soggetti che possano riferire sulla Segnalazione, qualora vi acconsentano espressamente.

Le suddette attività devono essere effettuate dal Comitato nel rispetto delle disposizioni previste dalle normative giuslavoristiche nazionali, dal Regolamento (UE) 2016/679 (di seguito, **GDPR**), dalla normativa nazionale in materia di protezione dei dati personali e dalla Norma e, per quanto occorrer possa, dal Modello di Organizzazione, Gestione e Controllo e dal Codice Etico adottati da SECURE NETWORK ai sensi del D. Lgs. n. 231/2001 e s.m.i..

Le Segnalazioni pervenute al Comitato sono classificate a seconda del loro contenuto e viene proposta l'archiviazione di quelle:

- generiche e/o non sufficientemente descritte e circostanziate;
- palesemente infondate o comunque non basate su elementi fattuali concreti;
- contenenti fatti già in precedenza oggetto di specifiche attività di verifica preliminari dalle quali non emergano nuove informazioni tali da rendere indispensabili ulteriori e nuove attività di verifica;
- non conformi alla Norma o alla Procedura ai sensi del precedente punto 6.

In caso di Segnalazioni che si riferiscano a uno o più membri del Comitato, tale/i componente/i si astiene/astengono dal partecipare alla verifica e agli accertamenti sulla specifica Segnalazione di Segn e viene/vengono sostituito/i dal/i membro/i supplente/i più anziano/i.

## **7.2 Accertamento**

Qualora, nel dar seguito alle Segnalazioni ricevute e all'esito delle opportune verifiche sugli elementi concreti forniti da Segn, il Comitato ritenga che la Segnalazione risulti fondata, in tutto o in parte, lo stesso, in relazione alla natura della Violazione, provvederà:

- a) a fornire un riscontro a Segn entro i termini previsti al punto 7.1. che precede;
- b) a comunicare l'esito dell'accertamento a Resp della BU della/e Persona/e coinvolta/e affinché, di concerto con HR e in ottemperanza alla Norma e alle leggi nazionali vigenti, adotti i provvedimenti ritenuti opportuni; in tal caso, Resp dovrà comunicare, per iscritto, i provvedimenti adottati di concerto con HR nei confronti della/e Persona/e coinvolta/e al Comitato e quest'ultimo lo comunica a Segn.

## **7.3 Conservazione della documentazione inerente alle Segnalazioni**

Le Segnalazioni e la relativa documentazione sono conservate per il tempo necessario al trattamento della Segnalazione stessa e comunque non oltre 5 (cinque) anni a decorrere dalla data del riscontro alla Segnalazione, nel rispetto degli obblighi di riservatezza di cui alla Norma e del principio di limitazione della conservazione dei dati personali di cui al GDPR e alla normativa nazionale applicabile alla protezione dei dati personali che dispone la cancellazione o l'anonimizzazione dei dati personali una volta conseguite le finalità per le quali sono stati trattati.

Quando, su richiesta di Segn, la Segnalazione è effettuata oralmente nel corso di un incontro con il Comitato, la medesima è documentata a cura del Comitato mediante registrazione su un dispositivo idoneo alla conservazione e all'ascolto oppure mediante redazione di un apposito verbale scritto. In quest'ultimo caso, Segn può verificare, rettificare e confermare il suo contenuto mediante la propria sottoscrizione.

## **8. TUTELA DELLA RISERVATEZZA**

Le Segnalazioni non possono essere utilizzate oltre quanto necessario per dare adeguato seguito alle stesse.

Tutti coloro che sono coinvolti a qualsiasi titolo nella gestione delle Segnalazioni sono specificamente formati e legati ad un vincolo che imponga loro di garantire la massima riservatezza su soggetti e fatti che ne formano oggetto. Con riferimento all'identità di Segn anonimo, è fatto loro espresso divieto di rivelare l'identità del medesimo a persone diverse da quelle specificamente autorizzate, in assenza del suo consenso espresso.

A Segn e a coloro che dichiarano di essere a conoscenza dei fatti oggetto della Segnalazione, è garantita la massima riservatezza in relazione alla propria identità, salvo qualora:

- essi dichiarino espressamente di acconsentire alla rivelazione;
- a carico di Segn sia accertata, anche con sentenza di primo grado, la responsabilità penale per calunnia o diffamazione o per reati comunque collegati alla Segnalazione ovvero la sua responsabilità civile, per lo stesso titolo, nei casi di dolo o colpa grave;
- Segn incorra in responsabilità extracontrattuale ai sensi dell'art. 2043 del Codice civile;
- in presenza di eventuali indagini o procedimenti avviati dall'Autorità Giudiziaria;

- si impone come necessario rivelare l'identità di Segn ai fini della prevenzione o della riduzione di minacce serie a danno della salute e/o della sicurezza delle persone.

Nell'ambito del procedimento disciplinare, l'identità di Segn non può essere rivelata, ove la contestazione dell'addebito disciplinare sia fondata su accertamenti distinti e ulteriori rispetto alla Segnalazione, anche se conseguenti alla stessa. Qualora la contestazione sia fondata, in tutto o in parte, sulla Segnalazione e la conoscenza dell'identità di Segn sia indispensabile per la difesa dell'incolpato, la Segnalazione sarà utilizzabile ai fini del procedimento disciplinare solo in presenza di consenso di Segn alla rivelazione della propria identità.

Il Comitato svolgerà un ruolo di vigilanza sul rispetto del divieto di atti di Ritorsione o discriminatori nei confronti di Segn e sul corretto utilizzo del canale interno di segnalazione.

Il Comitato, nella sua qualità di Titolare del trattamento ai sensi del GDPR, definisce il proprio modello di ricevimento e gestione delle Segnalazioni ed individua misure tecniche ed organizzative idonee a garantire un adeguato livello di sicurezza rispetto agli specifici rischi derivanti dai trattamenti effettuati sulla base di una valutazione di impatto sulla protezione dei dati personali ai sensi del GDPR e della normativa nazionale applicabile in materia.

La/e Persona/e coinvolta/e non ha/nno diritto ad ottenere le indicazioni circa l'origine della Segnalazione, né, tanto meno, di ricevere indicazioni circa i dati personali di Segn.

## **9. QUADRO NORMATIVO, MINIMIZZAZIONE DEL TRATTAMENTO, PROTEZIONE BY DESIGN E BY DEFAULT**

Ai sensi della Direttiva Whistleblowing e della Norma, al trattamento dei dati personali si applica il GDPR. Al riguardo, SECURE NETWORK applica i principi di liceità, correttezza e trasparenza, limitazione della finalità, minimizzazione dei dati, esattezza, limitazione della conservazione ed integrità e riservatezza relativi al trattamento dei dati personali e al principio della protezione dei dati fin dalla fase di concezione (c.d. *privacy by design*) e d'ufficio (c.d. *privacy by default*) definiti dal GDPR.

I dati personali che manifestamente non sono utili al trattamento di una specifica Segnalazione non sono raccolti e trattati dal Comitato o, se raccolti e trattati accidentalmente, sono cancellati senza indugio a cura del medesimo.

## **10. ALTRE FORME DI SEGNALAZIONE**

Segn può effettuare una segnalazione esterna (di seguito, **Segnalazione Esterna**) al canale appositamente attivato dall'Autorità Nazionale Anticorruzione (ANAC) ai sensi della Norma se, al momento della sua presentazione, ricorre una delle seguenti condizioni:

- a. Segn ha già effettuato una Segnalazione al canale di segnalazione interno attivato da SECURE NETWORK ai sensi della Norma (di seguito, **Segnalazione Interna**) e la stessa non ha avuto seguito;
- b. Segn ha fondati motivi di ritenere che, se effettuasse una Segnalazione Interna, alla stessa non sarebbe dato efficace seguito ovvero che la stessa Segnalazione possa determinare il rischio di Ritorsione;

- c. Segn ha fondato motivo di ritenere che la Violazione possa costituire un pericolo imminente o palese per il pubblico interesse.

Segn può effettuare la Segnalazione Esterna per iscritto tramite la piattaforma informatica messa a disposizione dall'ANAC oppure in forma orale attraverso linee telefoniche o sistemi di messaggistica vocale ovvero, su richiesta di Segn, mediante un incontro diretto.

Segn, oltre a poter effettuare una Segnalazione Interna e/o una Segnalazione Esterna, può effettuare una divulgazione pubblica (di seguito, **Divulgazione Pubblica**) se, in quel momento, ricorre una delle seguenti condizioni:

- a. Segn ha previamente effettuato una Segnalazione Interna ed Esterna e non è stato dato riscontro nei termini previsti dalla Norma;
- b. Segn ha fondato motivo di ritenere che la Violazione possa costituire un pericolo imminente o palese per il pubblico interesse;
- c. Segn ha fondato motivo di ritenere che la Segnalazione Esterna possa comportare il rischio di Ritorsioni o possa non avere efficace seguito in ragione delle specifiche circostanze del caso concreto, come quelle in cui possano essere occultate o distrutte prove oppure in cui vi sia fondato timore che chi ha ricevuto la Segnalazione possa essere colluso con la Persona coinvolta o coinvolto nella Violazione stessa.

## 11. MISURE DI PROTEZIONE PER SEGN

Le misure di protezione di Segn, previste dalla Norma ed applicabili ai soggetti che abbiano presentato una Segnalazione o una denuncia alle autorità preposte in presenza dei requisiti previsti dalla medesima Norma, comportano la nullità degli atti assunti ai sensi dell'art. 17 della Norma qualora essi possano essere riconosciuti come Ritorsioni.

Pertanto, costituiranno Ritorsioni, a titolo esemplificativo ma non esaustivo, i seguenti atti:

- il licenziamento, la sospensione o misure equivalenti;
- la retrocessione di grado o la mancata promozione;
- il mutamento di funzioni, il cambiamento del luogo di lavoro, la riduzione dello stipendio, la modifica dell'orario di lavoro;
- tutte le altre fattispecie previste dall'art. 17 della Norma e/o tutte quelle che saranno considerate tali dall'Autorità Giudiziaria adita.

## 12. SANZIONI

### 12.1 Le sanzioni dell'ANAC ai sensi della Norma

Fermi restando gli altri profili di responsabilità, in ossequio a quanto previsto dall'art. 21 della Norma, per coloro che si saranno resi responsabili delle seguenti violazioni l'ANAC può irrogare le seguenti sanzioni amministrative pecuniarie:

- a. **da € 10.000 a € 50.000**, qualora siano accertati (i) la commissione di Ritorsioni o (ii) comportamenti che hanno ostacolato o tentato di ostacolare le Segnalazioni o (iii) violazione dell'obbligo di riservatezza;
- b. **da € 10.000 a € 50.000**, qualora siano accertati (i) la mancata istituzione del canale di segnalazione o (ii) la mancata adozione di procedure per l'effettuazione e la gestione delle Segnalazioni o (iii) l'adozione di procedure non conformi ai dettami legislativi o (iv) il mancato espletamento dell'attività di verifica ed analisi delle Segnalazioni ricevute;
- c. **da € 500 a € 2.500**, nel caso di perdita delle tutele, salvo che Segn sia stato condannato, anche solo in primo grado, per i reati di diffamazione o calunnia o comunque per altri reati collegati alla denuncia sporta all'autorità adita.

## 12.2 Le sanzioni di SECURE NETWORK

Fermi i divieti di Ritorsione nei confronti di Segn previsti dalla Norma, SECURE NETWORK potrà irrogare sanzioni a causa delle condotte che seguono:

- a) in caso di violazioni della Procedura da parte dei soggetti posti in posizione "apicale", in quanto titolari di funzioni di rappresentanza, di amministrazione e di direzione di SECURE NETWORK o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale ovvero titolari del potere, anche solo di fatto, di gestione o di controllo di SECURE NETWORK;
- b) in caso di violazioni della Procedura da parte dei componenti degli organi di controllo e dei soggetti sottoposti all'altrui direzione o vigilanza o operanti in nome e/o per conto di SECURE NETWORK;
- c) in caso di violazioni delle tutele del/la dipendente che effettua la Segnalazione;
- d) qualora, a seguito di adeguata istruttoria da parte del Comitato, la Segnalazione si rivelasse infondata poiché effettuata con dolo o colpa grave da parte di Segn nonché in caso di dolo o colpa grave di Segn.

Le suddette condotte ledono il rapporto di fiducia instaurato con SECURE NETWORK e costituiscono altresì una violazione degli obblighi di diligenza e fedeltà del/della lavoratore/lavoratrice di cui agli artt. 2104 e 2105 del Codice civile. Pertanto, poiché le regole imposte dalla Procedura e, più in generale dal Modello di Organizzazione Gestione e Controllo e dal Codice Etico adottati da SECURE NETWORK ai sensi del D. Lgs. n. 231/2001 e s.m.i, cui la medesima si conforma, sono assunte da SECURE NETWORK in piena autonomia, indipendentemente dall'illecito che eventuali condotte possano determinare, l'applicazione delle sanzioni disciplinari prescinde dall'esito di un eventuale procedimento penale.

I nuovi precetti saranno soggetti alle garanzie procedurali di cui alla Legge n. 300/1970 e s.m.i. (di seguito, **Statuto dei Lavoratori**) ed alle specifiche disposizioni del Contratto Collettivo Nazionale del Lavoro applicato (di seguito, **CCNL**).

Il presente sistema disciplinare, oltre ad essere pubblicato sul sito web aziendale, è affisso presso le sedi di SECURE NETWORK, in luogo accessibile a tutti/tutte, affinché ne sia garantita la piena conoscenza da parte dei destinatari.

La tipologia e l'entità della sanzione saranno proporzionalmente individuate in relazione:

- all'intenzionalità del comportamento o al grado di negligenza, imprudenza o imperizia;
- al comportamento complessivo del soggetto autore dell'illecito disciplinare, con particolare riguardo alla sussistenza o meno di precedenti disciplinari del medesimo, nei limiti consentiti dalla legge;
- alle mansioni del soggetto autore dell'illecito disciplinare;

- alla posizione funzionale delle persone coinvolte nei fatti costituenti la mancanza;
- alle altre particolari circostanze che accompagnano la violazione disciplinare.

Il Comitato che presiede la Procedura, accertate eventuali violazioni, le comunica ad HR per l'avvio delle azioni necessarie. HR dovrà tenere informato il Comitato in merito all'esito del procedimento disciplinare.

### **12.3 Provvedimenti per i/le lavoratori/lavoratrici dipendenti di SECURE NETWORK**

I comportamenti tenuti dai/dalle lavoratori/lavoratrici in violazione delle singole regole comportamentali qui indicate sono definiti illeciti disciplinari. Le sanzioni irrogabili nei riguardi dei/delle lavoratori/lavoratrici sono quelle previste, nel rispetto delle procedure e dei limiti di cui all'art. 7 dello Statuto dei Lavoratori, dal CCNL di settore. Le singole fattispecie considerate e le sanzioni concretamente previste per la commissione dei fatti stessi assumono rilevanza a seconda della gravità della violazione. Le sanzioni astrattamente applicabili sono:

- richiamo verbale;
- ammonizione scritta;
- multa;
- sospensione dal lavoro e dalla retribuzione fino ad un massimo di 10 (dieci) giorni;
- licenziamento con preavviso;
- licenziamento senza preavviso.

Delle violazioni commesse devono essere informati i vertici societari di SECURE NETWORK affinché assumano le decisioni necessarie.

### **12.4 Misure nei confronti degli amministratori e dei soggetti apicali di SECURE NETWORK**

Tutti coloro che rivestono all'interno di SECURE NETWORK ruoli apicali hanno il dovere di orientare l'etica aziendale e di improntare la propria attività al rispetto dei principi di legalità, trasparenza e correttezza.

In caso di violazione della Procedura da parte degli amministratori e dei soggetti apicali di SECURE NETWORK, il Comitato è tenuto quanto prima ad informarne l'intero Consiglio di Amministrazione e l'intero Collegio Sindacale, i quali potranno assumere ogni opportuna iniziativa consentita dalla legge, tra cui le seguenti sanzioni:

- il richiamo scritto;
- la diffida al puntuale rispetto delle previsioni della Procedura;
- una sanzione pecuniaria;
- la revoca di eventuali procure.

Nelle ipotesi in cui le eventuali violazioni da parte degli Amministratori di SECURE NETWORK siano di tale gravità da compromettere il rapporto di fiducia tra il singolo soggetto e SECURE NETWORK, il Consiglio di Amministrazione convoca ai sensi dell'art. 2366 del Codice civile l'Assemblea ordinaria dei Soci di SECURE NETWORK al fine di proporre la revoca dall'incarico ai sensi degli artt. 2364, comma 1, n. 2) e 2383, comma 3, del Codice civile.

## **12.5 Misure nei confronti dei membri del Collegio Sindacale di SECURE NETWORK**

In caso di violazione della Procedura da parte dei membri del Collegio Sindacale, il Comitato è tenuto quanto prima ad informarne l'intero Consiglio di Amministrazione e l'intero Collegio Sindacale, i quali potranno assumere ogni opportuna iniziativa consentita dalla legge.

Nelle ipotesi in cui le eventuali violazioni siano di tale gravità da integrare una giusta causa di revoca ai sensi dell'art. 2400, comma 2, del Codice civile, il Consiglio di Amministrazione convoca ai sensi dell'art. 2366 del Codice civile l'Assemblea ordinaria dei Soci di SECURE NETWORK al fine di proporre i provvedimenti di competenza.

## **12.6 Misure nei confronti di collaboratori/trici esterni di SECURE NETWORK**

I comportamenti tenuti da lavoratori/lavoratrici autonomi/autonome (collaboratori/ collaboratrici occasionali, consulenti, ecc.) che contrastino con le linee di condotta indicate nella Procedura determineranno l'applicazione delle clausole contrattualmente previste (ad es. l'applicazione di penali e/o la risoluzione del contratto), nonché delle generali disposizioni di legge in materia di inadempimento e di giusta causa di recesso.

## **13. RINVIO**

Per tutto quanto non espressamente previsto dalla Procedura, si fa espresso rinvio alla Norma e alle norme nazionali applicabili in ragione della specificità della materia che ne forma oggetto.