amissima

ASSET MANAGEMENT
& INSURANCE SOLUTIONS

# MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO

*Decreto Legislativo 08 giugno 2001 n. 231*

***Testo deliberato dal Consiglio di Amministrazione***
***del 22 marzo 2018***

***Aggiornamento giugno 2018***

# INDICE

INDICE

# GLOSSARIO

Nel presente documento si intendono per:

- Aree a rischio: aree aziendali nell'ambito delle quali vengono svolte attività sensibili.
- Attività sensibili: attività di Amissima Holdings S.p.A. nel cui ambito sussiste il rischio della commissione dei reati previsti dalla normativa di riferimento (D. Lgs. 231/2001 e successive integrazioni).
- Amissima Holdings (o "Holding" o "Società" o "Capogruppo"): Amissima Holdings S.r.l., con sede legale in Milano, Viale Certosa, n. 222.
- Amissima Vita: Amissima Vita S.p.A., con sede legale in Genova, Via Mura di Santa Chiara, n. 1.
- Amissima Assicurazioni: Amissima Assicurazioni S.p.A., con sede legale in Milano, Viale Certosa, n. 222.
- CCNL: i Contratti Collettivi Nazionali di Lavoro stipulati da ANIA e dalle associazioni sindacali maggiormente rappresentative per il Personale, oltre che al Contratto Integrativo Aziendale, attualmente in vigore e applicati da Amissima Holdings.
- Consulenti o collaboratori esterni: soggetti che esercitano la loro attività in favore dell'azienda in forza di un rapporto contrattuale di collaborazione o di un mandato diverso da quello stipulato con la Rete Distributiva.
- D. Lgs. 231/2001 o il Decreto: il Decreto Legislativo n. 231 del 08 giugno 2001.
- Dipendenti o Personale Dipendente: soggetti legati da un rapporto di lavoro subordinato con Amissima Holdings (compresi i dirigenti) o da un rapporto contrattuale allo stesso assimilato (es. lavoratori a progetto).
- Distacco: Regime tramite il quale il Personale Dipendente delle Società Controllate opera per conto di Amissima Holdings, a fronte del ricevimento di una specifica Lettera di Distacco; nel testo anche Distaccati o Personale distaccato dalle Controllate o Regime di Distacco o Accordi di Distacco[1].
- Gruppo Assicurativo Amissima (o "Gruppo Assicurativo" o "Gruppo"): gruppo assicurativo iscritto all'Albo dei Gruppo Assicurativi presso IVASS con il numero d'ordine 050, composto

[1] Attualmente il Regime di Distacco è l'unico strumento tramite il quale i Dipendenti delle Controllate operano per conto della Controllante.

dalla Capogruppo Amissima Holdings S.r.l., dalle imprese assicuratrici Amissima Assicurazioni S.p.A. e Amissima Vita S.p.A., e dalle imprese strumentali Assi 90 S.r.l., I.H. Roma S.r.l. e Dafne Immobiliare S.r.l.

- Linee Guida ANIA: le Linee Guida dell'ANIA, adottate dalla Giunta Esecutiva dell'ANIA in data 26 novembre 2002 ed inviate alle imprese assicuratrici con la Circolare del 14 febbraio 2003, per la costruzione dei modelli di Organizzazione, Gestione e Controllo per il settore assicurativo (art. 6, comma 3, del D. Lgs. 231/2001).

- Linee Guida Confindustria: le Linee Guida di Confindustria, approvate dal Ministero della Giustizia con il Decreto Ministeriale del 4 dicembre 2003. L'ultima versione risale al 2014, questa approvata dal Ministero della Giustizia in data 21 luglio 2014, giudicando tali linee guida idonee al raggiungimento delle finalità previste dal Decreto 231.

- Modello o MOG: Modello di Organizzazione, Gestione e Controllo ai sensi del D. Lgs. 231 del 08 giugno 2001.

- Normativa di riferimento nazionale o Decreto: D. Lgs. 231 dell'8 giugno 2001 e successive modificazioni ed integrazioni.

- Organismo di Vigilanza o OdV: Organismo di Vigilanza previsto dal D. Lgs. 231/2001.

- Pubblica Amministrazione (P.A.): tutti gli enti pubblici, territoriali e non, i membri e gli organi interni degli enti, compresi i pubblici funzionari.

- Reati: novero dei reati previsti dal D. Lgs. 231/2001 e le successive modificazioni ed integrazioni.

- Successive integrazioni e modificazioni: per ogni normativa riportata (e.g. Legge, Decreto Legge, Decreto Legislativo, Disegno di Legge), si faccia sempre riferimento alle variazioni introdotte dalle specifiche successive integrazioni e modificazioni in vigore, apportate alla stessa.

- Società Controllate: le Società controllate direttamente da Amissima Holdings, cioè le Compagnie assicurative Amissima Vita e Amissima Assicurazioni, e le Società strumentali controllate in via indiretta, cioè le Società immobiliari Dafne S.r.l. e I.H. Roma S.r.l. e la Società di intermediazione assicurativa Assi 90 S.r.l.

- Vertice Aziendale o *Management* o Dirigenti: Alta Direzione di Amissima Holdings S.r.l.[2]

[2] Si intende il "*management*" delle Compagnie di Assicurazione che, avendo la responsabilità di Unità Organizzative operanti a livello di Gruppo, svolgono la propria mansione anche per la Società, in Regime di Distacco.

# PARTE GENERALE

## CAPITOLO 1 RIFERIMENTI NORMATIVI

### 1.1 Contenuto del D. Lgs. 231/2001 e normativa di riferimento

Il D. Lgs. 231/2001 del 08 giugno 2001 recante la "Disciplina della responsabilità amministrativa delle persone giuridiche, della Società e delle associazioni anche prive di personalità giuridica", entrato in vigore in data 04 luglio 2001, è stato emanato in esecuzione della delega concessa dal Parlamento al Governo di cui all'art. 11 della Legge 29 settembre 2000, n. 300.

Tale provvedimento normativo si è dimostrato necessario al fine di adeguare l'assetto normativo nazionale, in materia di responsabilità penale delle persone giuridiche, ad alcune disposizioni normative internazionali.

Le fonti di diritto internazionale a cui si fa riferimento, alle quali peraltro l'Italia aveva già aderito, si sostanziano nella:

- Convenzione di Bruxelles del 26 luglio 1995 "Tutela degli interessi finanziari delle Comunità Europee";
- Convenzione di Bruxelles del 26 maggio 1997 "Lotta alla corruzione in cui sono coinvolti funzionari della Comunità Europea e degli Stati Membri";
- Convenzione OCSE del 17 dicembre 1997 "Corruzione di Pubblici Ufficiali stranieri nelle operazioni economiche internazionali".

È noto come, prima della normativa poc'anzi citata, il brocardo latino "*societas delinquere non potest*" abbia condizionato anche il nostro Legislatore al punto tale che il principio della "personalità" della responsabilità penale (art. 25 della Costituzione) sia stato interpretato, dalla dottrina prevalente, come impossibilità di concepire una qualsivoglia responsabilità penale in capo alle persone giuridiche.

Il D. Lgs. 231/01, con l'art. 5 comma 1, statuisce la responsabilità della Società qualora determinati reati siano commessi, nell'interesse e a vantaggio della Società stessa, dai seguenti soggetti (c.d. "portatori di interesse della Società"):

- soggetti che rivestono ruoli di rappresentanza, amministrazione o di direzione della Società o di una sua unità organizzativa dotata di autonomia gestionale e finanziaria, nonché da soggetti che esercitano, anche in via di fatto, la gestione e il controllo della Società stessa;
- soggetti sottoposti alla direzione ed alla vigilanza dei soggetti sopra identificati.

Nello specifico, per "portatori di interesse della Società" devono intendersi:

- i Soci della Società;
- i membri dell'Organo Amministrativo individualmente considerati e l'Organo Amministrativo inteso a livello collegiale;
- i membri del Collegio Sindacale individualmente considerati e il Collegio Sindacale inteso collegialmente considerato;
- i Dipendenti della Società e i Distaccati delle Controllate;
- i Rappresentanti della Società, a qualunque titolo validamente costituita secondo le leggi italiane;
- i Collaboratori, a qualunque titolo, della Società.

Qualora uno dei soggetti sopra elencati ponga in essere un'attività criminosa, rientrante in una delle fattispecie previste dalla normativa di riferimento, alla responsabilità penale del soggetto agente andrà a sommarsi la responsabilità della Società, nel cui interesse o vantaggio l'attività stessa è stata posta in essere.

Alla Società sarà, infatti, comminata una sanzione pecuniaria e, nelle ipotesi di maggiore gravità, la normativa prevede l'ulteriore applicazione di sanzioni interdittive (come, a titolo puramente esemplificativo, l'interdizione dall'esercizio dell'attività, la sospensione o la revoca delle autorizzazioni, licenze e concessioni, il divieto di contrarre con la P.A., l'esclusione da agevolazioni, finanziamenti, contributi, sussidi o l'eventuale revoca di quelli già connessi, il divieto di pubblicizzare la fornitura di beni e servizi).

La responsabilità amministrativa della Società, tuttavia, non è *"legata"* alla commissione di qualsivoglia reato, ma può essere eventualmente configurata solo in relazione a quegli illeciti penali espressamente richiamati dal D. Lgs 231/2001 e dalla Legge n. 146/2006.

Invero, in ossequio al principio di legalità di cui all'art. 2 del D. Lgs 231/2001, per configurare una responsabilità riconducibile alla Società sono individuate come rilevanti solo specifiche tipologie di reati c.d. presupposto (di seguito, per brevità, anche i "Reati Presupposto"), al verificarsi dei quali è connessa la responsabilità diretta della Società.

Nel suo testo originario, il D. Lgs 231/2001 elencava tra i reati dalla cui commissione derivava la responsabilità amministrativa delle società, esclusivamente quelli nei confronti della Pubblica Amministrazione e quelli contro il patrimonio, commessi a danno dello Stato o di altro ente pubblico (artt. 24 e 25 del Decreto 231).

Successivamente, l'elencazione dei reati presupposto della responsabilità amministrativa delle società è stata notevolmente ampliata (le ultime integrazioni del catalogo dei reati-presupposto sono state operate per effetto dell'entrata in vigore della Legge 20 novembre 2017 n. 167 che ha introdotto il delitto di Razzismo e xenofobia all'art. 25 *terdecies*, del D. Lgs. n. 231/2001).

Attualmente, i reati-presupposto della responsabilità amministrativa dell'Ente sono riconducibili alle categorie di seguito indicate:

1. Indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di un ente pubblico (art. 24, D. Lgs. n. 231/2001);
2. Delitti informatici e trattamento illecito di dati (art. 24-bis, D. Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 48/2008; modificato dal D. Lgs. n. 7 e 8/2016];
3. Delitti di criminalità organizzata (art. 24-ter, D. Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 94/2009 e modificato dalla L. 69/2015];
4. Concussione, induzione indebita a dare o promettere altra utilità e corruzione (art. 25, D. Lgs. n. 231/2001) [articolo modificato dalla L. n. 190/2012];
5. Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (art. 25-bis, D. Lgs. n. 231/2001) [articolo aggiunto dal D.L. n. 350/2001, convertito con modificazioni dalla L. n. 409/2001; modificato dalla L. n. 99/2009; modificato dal D. Lgs. 125/2016];
6. Delitti contro l'industria e il commercio (art. 25-bis.1, D. Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 99/2009];

7. Reati societari (art. 25-ter, D. Lgs. n. 231/2001) [articolo aggiunto dal D. Lgs. n. 61/2002, modificato dalla L. n. 190/2012, dalla L. 69/2015 e dal D. Lgs. n.38/2017];
8. Reati con finalità di terrorismo o di eversione dell'ordine democratico previsti dal codice penale e dalle leggi speciali (art. 25 *quater*, D. Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 7/2003];
9. Pratiche di mutilazione degli organi genitali femminili (art. 25 *quater*.1, D. Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 7/2006];
10. Delitti contro la personalità individuale (art. 25 *quinquies*, D. Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 228/2003; modificato dalla L. n. 199/2016];
11. Reati di abuso di mercato (art. 25 *sexies*, D. Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 62/2005];
12. Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro (art. 25-*septies*, D. Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 123/2007];
13. Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché auto-riciclaggio (art. 25 *octies*, D. Lgs. n. 231/2001) [articolo aggiunto dal D. Lgs. n. 231/2007; modificato dalla L. n. 186/2014];
14. Delitti in materia di violazione del diritto d'autore (art. 25 *novies*, D. Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 99/2009];
15. Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25 *decies*, D. Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 116/2009];
16. Reati ambientali (art. 25 *undecies*, D. Lgs. n. 231/2001) [articolo aggiunto dal D. Lgs. n. 121/2011, modificato dalla L. n. 68/2015];
17. Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 25 *duodecies,* D. Lgs. n. 231/2001) [articolo aggiunto dal D. Lgs. n. 109/2012, modificato dalla Legge 17 ottobre 2017 n. 161];
18. Razzismo e xenofobia (art. 25 *terdecies*, D. Lgs. n. 231/2001) [articolo aggiunto dalla Legge 20 novembre 2017 n. 167];

19. Responsabilità degli enti per gli illeciti amministrativi dipendenti da reato (art. 12, L. n. 9/2013) [Costituiscono presupposto per gli enti che operano nell´ambito della filiera degli oli vergini di oliva];
20. Reati transnazionali (L. n. 146/2006) [Costituiscono presupposto per la responsabilità amministrativa degli enti i seguenti reati se commessi in modalità transnazionale].

L'Allegato 1 riporta un elenco dettagliato dei reati presupposto vigenti al momento della approvazione del presente documento. Il predetto elenco, quale parte integrante del Modello, sarà aggiornato, eventualmente, nel rispetto di quanto previsto dalla presente Parte Generale.

### 1.2 I principi di esclusione della responsabilità dell'ente

Il D. Lgs. 231/2001 prevede, agli artt. 6 e 7, la possibilità per le persone giuridiche di essere esenti da responsabilità nel caso in cui provvedano ad adottare "modelli di organizzazione, gestione e controllo" atti a prevenire la commissione dei reati inclusi nel suddetto catalogo.
I modelli devono rispondere alle seguenti esigenze:

- prevedere una preliminare "mappatura" delle aree di rischio nell'ambito delle quali risulta possibile la commissione di reati;
- tracciare adeguate procedure che abbiano, come specifica caratteristica, l'essere pensate ed attuate anche al fine di prevenire la commissione di reati;
- individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione di reati;
- prevedere l'istituzione di un Organismo di Vigilanza interno all'ente con il compito di monitorare l'allineamento dell'azienda ai protocolli operativi, verificare l'efficacia dei codici comportamentali e provvedere al relativo aggiornamento laddove necessario;
- prevedere obblighi di informazione a favore dell'Organismo di Vigilanza;
- prevedere l'introduzione di un sistema disciplinare idoneo a sanzionare il mancato rispetto delle regole proprie del Modello approvato (l'autore del reato deve aver agito eludendo fraudolentemente le disposizioni del Modello);

- prevedere un sistema di verifica periodica e di eventuale aggiornamento del Modello.

Il D. Lgs. 231/2001 prevede, inoltre, che la Società possa adottare un Modello sulla base di codici di comportamento elaborati da associazioni di categoria e comunicati al Ministero della Giustizia che, entro 30 giorni dal ricevimento degli stessi può formulare, di concerto con gli altri Ministeri interessati, osservazioni sull'idoneità del Modello stesso.

### 1.3 Le linee guida

Nell'elaborazione del Modello di Organizzazione, Gestione e Controllo, Amissima Holdings S.p.A. si è ispirata alle Linee Guida emanate dall'ANIA, per il settore assicurativo, ed in quanto applicabili, anche in considerazione del loro più recente aggiornamento, alle linee guida emanate da Confindustria.

L'ANIA, in ossequio al dettato normativo di cui all'art. 6 del D, Lgs. 231/2001, indica i punti fondamentali per la costruzione del Modello, ossia:

a) individuazione delle cc. dd. "aree di rischio", ovvero l'analisi dell'operatività aziendale al fine di verificare quali siano le attività nell'ambito delle quali possano verificarsi i reati previsti dal decreto;
b) progettazione del sistema di controllo attraverso l'implementazione di opportuni protocolli ovvero attraverso la verifica del sistema esistente, in termini di riduzione, ad un livello accettabile[3], del rischio di commissione degli eventi pregiudizievoli come sopra identificati;
c) obblighi di informazione dell'Organismo di Vigilanza, volti a soddisfare l'attività di controllo sul funzionamento, sull'efficacia e l'osservanza del Modello.

Le componenti di maggiore importanza del sistema di controllo sono state individuate nei seguenti strumenti:

- Elaborazione di codici di comportamento e di condotta;
- Implementazione di un sistema organizzativo;
- Individuazione dei poteri autorizzativi e di firma;

[3] Vale a dire individuare quei controlli che, seppur senza azzerare il rischio, consentono di limitare lo stesso ad un livello tale per cui qualsiasi ulteriore azione di controllo "costerebbe" (in termini economici e di perdita di efficacia del sistema organizzativo aziendale) più della risorsa da proteggere.

- Implementazione di un sistema di controllo e di gestione;
- Erogazione di formazione ed informazione al personale e a tutti i soggetti operanti nel contesto aziendale;
- Adozione di meccanismi disciplinari.

Le componenti del sistema di controllo interno devono rispettare i seguenti principi:

- Verificabilità, tracciabilità, coerenza e congruenza di ogni operazione;
- Applicazione del principio di separazione delle funzioni (c.d. *four eyes principle*: la funzione che dispone l'operazione è diversa dalla funzione incaricata dell'approvazione/verifica della stessa);
- Tracciabilità dei controlli previsti;
- Previsione di un adeguato sistema sanzionatorio in caso di violazione delle regole e delle procedure previste dal Modello;
- Individuazione dei requisiti dell'Organismo di Vigilanza, quali autonomia ed indipendenza, professionalità e continuità di azione.

Per quanto riguarda la dinamica dei Gruppi Assicurativi, è la stessa ANIA a puntualizzare la necessità che ogni compagnia inserita nell'ambito di un gruppo mantenga, comunque, la propria autonomia e debba, conseguentemente, dotarsi di un autonomo sistema di controllo. È possibile, comunque, individuare delle linee comuni alle quali uniformare i modelli di Organizzazione, Gestione e Controllo di tutte le realtà facenti parte del gruppo.

Si evidenzia che, come richiesto dalle *best practices* e dalle linee guida stesse il Modello è stato redatto con riferimento alla realtà operativa concreta della Società e del Gruppo Assicurativo Amissima dunque il medesimo si può discostare dalle linee guida considerate che per loro natura hanno carattere generale e standardizzato.

# CAPITOLO 2 IL GRUPPO AMISSIMA

## 2.1 Composizione del Gruppo e ruolo di Amissima Holdings

Amissima Holdings S.r.l. è Capogruppo del Gruppo Assicurativo Amissima, iscritto nell'apposito Albo dei Gruppi con il numero 050 con provvedimento IVASS n. 0139886 il 7 ottobre 2015.

Fanno parte del Gruppo Amissima le seguenti società:

- Amissima Holdings S.r.l., Società Capogruppo con sede in Milano;
- Amissima Vita S.p.A., Società con sede in Genova, che esercita l'attività di assicurazioni sulla Vita ed è controllata al 100% da Amissima Holdings S.r.l.;
- Amissima Assicurazioni S.p.A., Società con sede in Milano, che esercita l'attività di assicurazioni nei Rami Danni ed è controllata da Amissima Holdings al 100% S.r.l.;
- Dafne Immobiliare S.r.l., Società immobiliare controllata al 100% da Amissima Assicurazioni S.p.A.;
- I.H. Roma S.r.l., Società immobiliare controllata al 100% da Amissima Vita S.p.A.;
- Assi 90 S.r.l., Società di intermediazione assicurativa controllata al 60,25% da Amissima Vita S.p.A. e partecipata al 39,75% da Amissima Assicurazioni S.p.A.

Amissima Holdings S.r.l. in qualità di impresa italiana di partecipazione assicurativa e riassicurativa esercita un controllo diretto sulle Imprese di Assicurazione Amissima Vita S.p.A. e Amissima Assicurazioni S.p.A. ed un controllo indiretto sulle società strumentali Assi 90 S.r.l., I.H. Roma S.r.l. e Dafne S.r.l.

### *2.1.1 Amissima Holdings S.r.l.*

La Società ha per oggetto l'assunzione, gestione e valorizzazione di partecipazioni di controllo, principalmente, in imprese di assicurazione italiane, comunitarie o extracomunitarie nonché, in imprese di riassicurazione, esercitando il coordinamento tecnico, finanziario e amministrativo nei confronti dei soggetti del Gruppo Amissima, nonché, svolgendo nei confronti di questi l'attività di indirizzo e controllo strategico, gestionale, operativo.

La Società è Capogruppo del Gruppo Assicurativo Amissima ed è soggetta ai controlli di vigilanza imposti dall'IVASS in conformità alle disposizioni del Codice delle Assicurazioni private, oltre a dover adottare, nell'esercizio dell'attività di direzione e coordinamento nei confronti delle società partecipate, i provvedimenti per l'attuazione delle disposizioni impartite dall'IVASS.

In considerazione di quanto sopra, la Società ha istituito, in modalità accentrata presso di sé, le seguenti funzioni: Attuariale; *Risk Management*; *Internal Audit*; *Compliance*, nonché, Antiriciclaggio e Antiterrorismo, ferma restando la presenza di tali funzioni in entrambe le Compagnie di Assicurazione.

Tale accentramento è stato regolamentato tramite contratti infragruppo per singola funzione, tra la Società e le singole controllate. Tali contratti sono stati approvati dall'Organo Amministrativo ed inviati a IVASS ai fini della relativa efficacia.

Viceversa, al fine di razionalizzare le competenze evitando al contempo una duplicazione di costi, le funzioni c.d. "trasversali" o di "supporto" - quali, Amministrazione; Servizi Generali; Legale; Segreteria Societaria; Gestione del Personale; Normativa Aziendale, Sistemi Informatici/Organizzazione e Segreteria di Direzione – sono svolte in favore della Società dalle risorse delle controllate sulla base di appositi accordi di distacco. Il Personale Dipendente e il Personale Distaccato dalle Controllate ricevono dagli Organi di gestione di Amissima Holdings S.r.l. specifiche indicazioni ed indirizzi operativi in merito alle attività che, nel ruolo ricoperto, la risorsa è tenuta a svolgere ed alle modalità operative che la stessa deve adottare nell'ambito del contesto organizzativo e di governo della Holding.

### *2.1.2 L'assetto di governance della Società*

Amissima Holdings S.r.l. adotta un sistema di amministrazione e controllo di tipo "tradizionale" ai sensi degli artt. 2380 *bis* e seguenti del Codice Civile.

L'assetto di *governance* è fondato sui seguenti Organi:

- Assemblea dei Soci: è l'Organo che esprime con le sue deliberazioni la volontà degli azionisti; le adunanze assembleari sono il luogo privilegiato per l'instaurazione di un proficuo dialogo tra i Soci e gli Amministratori alla presenza del Collegio Sindacale;
- Consiglio di Amministrazione, nominato dall'Assemblea dei Soci, è l'Organo che presiede le scelte strategiche, le politiche aziendali e la definizione degli obiettivi sociali, ad esso è affidata la gestione aziendale per il conseguimento dell'oggetto sociale. Al Consiglio di Amministrazione fanno capo le funzioni e le inerenti responsabilità in materia di indirizzi strategici ed organizzativi, nonché la verifica dell'esistenza dei controlli necessari per garantire la correttezza e la legittimità dell'operato della Società.
- Presidente del Consiglio di Amministrazione e Amministratore Delegato, al quale sono conferite specifiche deleghe di poteri ai sensi delle disposizioni di legge e di Statuto.
- Collegio Sindacale, è l'Organo avente funzioni di vigilanza sull'osservanza della legge e dello Statuto, nonché di controllo sulla gestione. Il Collegio Sindacale, nell'ambito dei compiti ad esso affidati dalla legge, vigila, avvalendosi delle strutture di controllo aziendali sul concreto funzionamento del sistema di controllo interno e verifica l'adeguatezza dell'assetto organizzativo, amministrativo e contabile approvato dal Consiglio di Amministrazione, a cui segnala eventuali anomalie o debolezze.

### *2.1.3 L'assetto organizzativo e di controllo interno*

L'impostazione organizzativa del Gruppo è volta ad una piena integrazione operativa tra tutte le società al fine di garantire:

- una univoca ed efficace *corporate* e *risk governance,* anche attraverso la coincidenza dei membri degli organi sociali;
- l'univocità, l'efficacia e l'efficienza dei processi e del controllo interno e di gestione dei rischi;
- l'attendibilità e l'integrità delle informazioni contabili e gestionali a livello individuale e consolidato;

- la salvaguardia del patrimonio della singola Società e del Gruppo;
- il pieno presidio dei principi etici e di sana e prudente gestione, la conformità dell'attività alla normativa vigente, alle direttive e alla normativa interna.

Nel seguito sono rappresentati i principali elementi che caratterizzano l'assetto organizzativo e di controllo definito da Amissima Holdings per il Gruppo Assicurativo:

*Codici Etici e di comportamento di Gruppo*

Il Gruppo Amissima si è dotato di un Codice Etico di Gruppo che si coordina con Codici Etici delle singole società (Amissima Holdings, Amissima Assicurazioni e Amissima Vita).

I Codici Etici, approvati dai rispettivi Consigli di Amministrazione, richiedono esplicitamente a tutti i soggetti apicali, ai dipendenti, ai portatori d'interesse e ai collaboratori la tenuta di comportamenti eticamente incensurabili, oltre che legalmente e professionalmente corretti, operando con integrità ed onestà internamente, con le società del Gruppo, con gli azionisti, con i clienti ed in genere con i terzi.

*Centralizzazione delle funzioni di controllo*

Le Funzioni di Controllo *Internal Audit*, *Compliance*, *Risk Management* e Antiriciclaggio/ Antiterrorismo e la Funzione Attuariale sono state istituite in modalità accentrata presso la Holding. Tale accentramento è regolamentato tramite contratti infragruppo, mediante i quali vengono individuati, nelle imprese cedenti, i referenti interni con il compito di fornire collaborazione al personale deputato dall'impresa cessionaria per lo svolgimento dell'attività oggetto di cessione, al fine di garantire adeguati ed uniformi standard, e che le politiche di valutazione e monitoraggio dei rischi definite dalla Holding siano adeguate per le caratteristiche operative delle società controllate.

Per garantire i prescritti caratteri di indipendenza, autonomia e autorevolezza, i Responsabili delle funzioni di controllo dipendono funzionalmente dall'Organo Amministrativo di Amissima Holdings al quale forniscono una periodica informativa delle attività di controllo svolte nell'ambito della Holding stessa e delle altre società del Gruppo.

*Linee guida e politiche di Gruppo*

Amissima Holdings emana ed aggiorna periodicamente linee guida (c.d. Politiche di Gruppo) inerenti gli assetti organizzativi, di governo e di controllo del Gruppo anche in considerazione delle disposizioni di Vigilanza applicabili al settore assicurativo.

Nell'ambito del perimetro del Gruppo Assicurativo, il Consiglio di Amministrazione della Holding ha adottato una serie di Linee Guida in materia di:

- Governance, Sistema dei Controlli Interni e conferimento delle Deleghe e dei Poteri;
- Requisiti di onorabilità, professionalità e indipendenza di Amministratori, Sindaci e Responsabili delle Funzioni di controllo e dei referenti interni della Società;
- *Internal Audit, Risk Management, Compliance*, Funzione attuariale, Antiriciclaggio e antiterrorismo;
- Valutazione attuale e prospettica dei rischi nell'ambito del Gruppo Assicurativo;
- Gestione del capitale su un orizzonte temporale di medio termine (non inferiore a 3 anni);
- Concentrazione dei rischi a livello di Gruppo;
- Gestione dei conflitti di interesse del Gruppo Assicurativo;
- Anticorruzione;
- Normativa interna;
- Esternalizzazione di attività del Gruppo Assicurativo;
- Operatività infragruppo;
- Gestione degli investimenti;
- Remunerazione;
- Segnalazioni destinate a Ivass;
- Dati e Informazioni Statistiche;
- Gestione SFCR – RSR;
- Valutazione attività e Passività.

I contenuti di tutte le linee guida sono recepite da parte delle Società Controllate.

*Monitoraggio dell'attività di Gruppo e flussi informativi*

Il Gruppo Amissima ha adottato e reso operativo un sistema di coordinamento informativo dalle controllate verso la Capogruppo mediante la definizione di flussi informativi periodici atti a verificare il perseguimento degli obiettivi definiti dalla Holding. Tali flussi sono stati disciplinati tramite apposita delibera del Consiglio di Amministrazione di Amissima Holdings S.r.l.[4]; la deliberazione assunta dalla Capogruppo Assicurativa è stata poi recepita dagli Organi Amministrativi delle Compagnie di Assicurazione.

Tale sistema di flussi informativi consente sia di verificare il perseguimento di obiettivi strategici e il rispetto della normativa, sia di monitorare e controllare le diverse operazioni che possano coinvolgere le imprese appartenenti al Gruppo.

La casistica dei flussi informativi periodici che le società facenti parte del Gruppo sono tenute ad inviare alla Holding, in qualità di capogruppo, con una cadenza prestabilita (e comunque almeno trimestrale) e/o ad evento, è relativa agli ambiti di seguito indicati:

a) ***Governance*** – è previsto l'obbligo in capo alle società del Gruppo di trasmettere alla capogruppo informazioni relative a statuto sociale, codice etico, composizione degli organi sociali, ordine del giorno delle sedute degli organi amministrativi e relativi verbali, operazioni con parti correlate, operazioni di maggior rilievo, elenco partecipazioni.

b) **Organizzazione aziendale** - è previsto l'obbligo in capo alle società del Gruppo di trasmettere alla Capogruppo informazioni relative a manuale organizzazione, funzionigramma e organigramma aziendale, modifiche dei documenti aziendali, siti internet, poteri di firma e rappresentanza, struttura dei processi ed elenco delle procedure in vigore (ove adottate), modello organizzativo ex D. Lgs. 231/01, principali contratti di *outsourcing*.

c) **Informazioni amministrative e finanziarie** - la Capogruppo, nel quadro dell'attività di direzione e coordinamento del Gruppo, eserciterà un controllo gestionale volto ad assicurare il mantenimento delle condizioni di equilibrio economico, finanziario e patrimoniale sia a livello individuale che di Gruppo; è, pertanto, previsto l'obbligo in capo a tutte le società del Gruppo

[4] Nel corso della seduta del 30 giugno 2015.

di trasmettere alla capogruppo, secondo tempistiche e modalità definite, i seguenti flussi contabili:

- Bilancio Annuale;
- Relazione Semestrale;
- Piani operativi e di *budget*.

d) **Informative verso gli Organi Sociali** - le società facenti parte del Gruppo devono fornire al Consiglio di Amministrazione della capogruppo preventiva informativa in merito ad ogni avvicendamento in seno agli organi amministrativi, di controllo e direzione.

e) **Operazioni di significativo rilievo strategico** – tali operazioni devono essere previamente sottoposte al Consiglio di Amministrazione della Capogruppo. A tal fine, è stata individuata una soglia di rilevanza oltre la quale le società facenti parte del Gruppo sono tenute ad ottenere il preventivo consenso della Capogruppo.

f) **Disposizioni in tema di operazioni con controparti infragruppo** - la Capogruppo ha definito una policy di Gruppo finalizzata a identificare:

- le controparti delle operazioni infragruppo;
- le tipologie delle operazioni infragruppo;
- le linee guida che governano le operazioni di natura assuntiva e non assuntiva;
- la disciplina degli obblighi informativi inerenti tali operazioni;
- norme procedurali interne e aspetti interpretativi.

g) ***Projects Management*** - sono portati all'attenzione della Capogruppo i fabbisogni delle singole entità del Gruppo in termini di risorse umane e di nuovi progetti di organizzazione finalizzati alla crescita del comparto assicurativo e al perseguimento di sinergie derivanti dall'utilizzo di infrastrutture tecnologiche comuni.

h) **Pianificazione strategica e controllo di gestione** - le società facenti parte del Gruppo devono fornire alla capogruppo un flusso dei dati relativamente al proprio andamento tecnico gestionale, mediante la predisposizione periodica di budget e reporting direzionali.

*Documentazione integrata della struttura organizzativa*

La struttura organizzativa del Gruppo è rappresentata in modo completo ed esaustivo tramite organigrammi e funzionigramma, comunicazioni organizzative, contratti infragruppo e lettere di distacco.

Tale set documentale consente di individuare chiaramente tutte le unità organizzative e le relative mission e responsabilità, i riporti gerarchici e funzionali.

*Sistema delle deleghe*

Il Sistema delle Deleghe del Gruppo è definito sulla base dalla Politica di Gruppo emanata dalla stessa Amissima Holdings, in coerenza con l'Organigramma di Amissima Holdings e il Funzionigramma Generale, al fine di garantire:

- una chiara identificazione ed una specifica assegnazione dei poteri e limiti ai soggetti che operano impegnando la Società e manifestando la volontà aziendale;
- la coerenza dei poteri attribuiti con le responsabilità organizzative assegnate;
- meccanismi adeguati di rendicontazione periodica dei poteri delegati.

*Sistema Normativo interno integrato*

Il sistema complessivo delle regole interne del Gruppo è istituito per disciplinare in modo chiaro, congruo ed esaustivo tutte le modalità operative rilevanti.

Le Politiche, emanate da Amissima Holdings ed adottate dalle società controllate, definiscono gli indirizzi in materia di *governance*, organizzazione e controllo interno e gestione dei rischi ed in merito alle attività di *core business*.

Le procedure e gli altri strumenti normativi regolamentano in modo adeguato i processi ed i flussi di lavoro:

- individuando le modalità operative, i flussi informativi;
- garantendo la documentazione formale delle attività e la loro ricostruibilità *ex post* nonché il monitoraggio e controllo di linea;
- individuando chiaramente la responsabilità del processo;

- garantendo la segregazione dei compiti e delle responsabilità;
- garantendo l'accessibilità e la conoscenza attraverso adeguate attività di informazione e formazione sulle normative aziendale.

*Sistema di controllo interno integrato*

Il Gruppo Amissima è dotato di un sistema di controllo interno definito a livello di Gruppo sulla base delle disposizioni emanate da Amissima Holdings e conseguentemente declinato in meccanismi di controllo specifico che pervadono l'intera operatività aziendale.

Il sistema di controllo interno include, tra l'altro, controlli sulla tracciabilità e sulla documentazione delle operazioni finanziarie effettuate, sulla coerenza con i poteri e le responsabilità assegnate, nonché sull'effettiva destinazione delle risorse a finalità coerenti con gli obiettivi aziendali e con i valori di correttezza, integrità e rispetto delle normative vigenti.

In coerenza con le *best practices* di riferimento e con le disposizioni di Vigilanza applicabili al comparto assicurativo, il sistema di controllo interno del Gruppo è impostato su 3 livelli:

- *Controlli di primo livello* (*c.d. controlli di linea*), ossia controlli di carattere sistematico effettuati dalle singole unità organizzative, delle società controllate nell'ambito dei processi aziendali di propria competenza; tali attività di controllo sono demandate alla responsabilità primaria del *management* e sono considerate parte integrante di ogni processo aziendale;
- *Controlli di secondo livello* (*c.d. controllo di gestione dei rischi*), ossia controlli affidati a unità organizzative diverse da quelle operative. Le unità organizzative responsabili dei controlli di 2° livello sono la Funzione *Risk Management*, *Compliance*, Antiriciclaggio e Antiterrorismo, e Attuariale;
- *Controlli di terzo livello* (*c.d. internal audit*), condotti da struttura diversa da quelle produttive e di controllo di 2° livello, ossia dalla Funzione di *Internal Audit*.

Le funzioni di controllo, nel rispetto delle disposizioni applicabili svolgono le seguenti principali funzioni:

- La Funzione *Risk Management*, garantisce l'indirizzo strategico e la definizione delle politiche di gestione del rischio, definisce i criteri per la valutazione, gestione, misurazione, monitoraggio e comunicazione di tutti i rischi a livello di Gruppo;
- La Funzione *Compliance*, presidia i rischi di non conformità alle norme di legge, di vigilanza e di autoregolamentazione, con particolare attenzione ai profili di trasparenza e correttezza contrattuale di tutela del consumatore e di impatto reputazionale;
- La Funzione Antiriciclaggio e Antiterrorismo assicura il rispetto delle disposizioni normative in materia di antiriciclaggio, monitorando i rischi di riciclaggio e di finanziamento del terrorismo a livello di Gruppo;
- La Funzione Attuariale coordina il calcolo delle riserve tecniche delle Compagnie assicurative, garantendone l'adeguatezza delle metodologie, dei modelli utilizzati e valutando la sufficienza e la qualità dei dati utilizzati per il calcolo ed analizzando e valutando tecnicamente i rischi del dominio di competenza del Gruppo coperti dal modello interno adottato dalle Imprese di Assicurazione.
- La Funzione di *Internal Audit* ha il compito di fornire *assurance* indipendente sulla completezza, funzionalità e adeguatezza del sistema dei controlli interni e gestione dei rischi a livello di Gruppo.

La responsabilità circa il funzionamento e la coerenza complessiva del sistema di controllo compete al Consiglio di Amministrazione di ogni Società del Gruppo che è tenuta ad applicare le disposizioni a tal fine emanate da Amissima Holdings.

I Consigli di Amministrazione, anche sulla base di informative periodiche da parte dell'Alta Direzione e dell'Organo di Controllo, svolgono un'attività periodica di valutazione della funzionalità, efficacia ed efficienza del sistema di controllo interno, adottando tempestivamente eventuali misure correttive al verificarsi di carenze e/o anomalie.

Il Collegio Sindacale di ogni Società del Gruppo esercita le funzioni previste dall'art. 2403 del Codice Civile e, anche nell'ambito delle prerogative attribuite dalla Normativa di Vigilanza, ha il compito di:

- verificare l'adeguatezza dell'assetto organizzativo, amministrativo e contabile adottato dall'Impresa e il suo concreto funzionamento;
- valutare l'efficienza e l'efficacia del sistema dei controlli interni, anche riguardo all'operato della funzione di *Internal Audit* della quale deve verificare la sussistenza della necessaria autonomia, indipendenza e funzionalità.

L'Alta Direzione è responsabile dell'attuazione, del mantenimento e del monitoraggio del sistema dei controlli interni e di gestione dei rischi, ivi compresi quelli derivanti dalla non conformità alle norme, coerentemente con le direttive dell'Organo Amministrativo.

Amissima Holdings S.r.l., nell'ottica di garantire un complessivo governo dei rischi ha costituito un apposito Comitato Rischi a livello di Gruppo, composto oltre che dai Responsabili delle Funzioni di Controllo anche da taluni rappresentanti del *Management*, che ha l'obiettivo di:

- valutare l'efficacia e migliorare la *governance* dei rischi, comprese le strategie, le politiche e i limiti e la propensione al rischio sia in ottica attuale che prospettica;
- valutare l'efficacia e il miglioramento del processo di gestione dei rischi rispetto alle caratteristiche del gruppo e del profilo di rischio assunto così come il suo effettivo funzionamento;
- supportare il Consiglio di Amministrazione nella valutazione della coerenza tra le linee di indirizzo del sistema di controllo interno e di gestione dei rischi con il modello di business e la propensione al rischio, dallo stesso definiti.

# CAPITOLO 3 ADOZIONE DEL MODELLO DA PARTE DI AMISSIMA HOLDINGS S.r.l.

## 3.1 Finalità del Modello

Amissima Holdings S.r.l. si dota del presente Modello di Organizzazione, gestione e controllo con l'obiettivo di prevenire la commissione dei reati previsti dal Decreto da parte di esponenti della Compagnia, apicali o sottoposti alla direzione altrui.

La Società considera fondamentale l'esigenza di assicurare condizioni di correttezza, legalità e trasparenza nella conduzione delle attività aziendali anche a tutela della propria reputazione e credibilità nei confronti degli *stakeholders*, cioè di coloro che contribuiscono o hanno, comunque, un interesse al conseguimento della missione aziendale, nonché dei singoli, organizzazioni ed istituzioni i cui interessi possono essere influenzati, in misura maggiore o minore, dall'operato della Società: azionisti, clienti, fornitori, collaboratori, organizzazioni politiche e sindacali, pubbliche amministrazioni e in generale, ambiente socio – economico.

L'articolo 6 comma 2, D. Lgs. 231/2001, inoltre, prevede che l'ente non risponde se l'apicale o il subordinato ha agito nell'interesse esclusivo proprio o di terzi, ovvero, qualora sia stato adottato un modello di organizzazione interna, dotato dei requisiti minimi previsti dalla legge. La sussistenza di un modello astrattamente 'idoneo' e concretamente 'attuato' esclude il coinvolgimento della Società, lasciando permanere la sola responsabilità della persona fisica che, eludendone fraudolentemente i protocolli, ha realizzato la fattispecie criminosa.

Pertanto, la funzione primaria del Modello di Amissima Holdings S.r.l. è quella di costituire un sistema strutturato ed organico atto a prevenire la commissione di reati previsti dal Decreto:

- vietando espressamente comportamenti che possano integrare fattispecie di reato di cui al Decreto;
- diffondendo a tutti i livelli della struttura la consapevolezza che, dalla violazione del Decreto e delle prescrizioni del Modello e del Codici Etici possono derivare misure sanzionatorie anche a carico della Società;

- diffondendo una cultura d'impresa improntata alla legalità e riprovando espressamente ogni comportamento contrario alla legge, ai regolamenti, e alle disposizioni anche interne contenute nel Modello stesso, nel Codici Etici e/o nelle normative aziendali ad essi riconducibili;
- dando evidenza di una struttura organizzativa efficace e coerente con l'assetto organizzativo adottato con particolare riferimento alla chiara attribuzione di poteri, alla formazione delle decisioni e alla loro trasparenza e motivazione, ai controlli sugli atti e le attività e alla correttezza dei flussi informativi interni ed esterni;
- consentendo, tramite il sistema di controllo e una costante azione di monitoraggio sulla corretta attuazione dello stesso, di prevenire e/o contrastare tempestivamente, la commissione di reati previsti dal Decreto.

### 3.2 Destinatari del Modello

Le regole contenute nel presente Modello si rivolgono a:

a. coloro che ricoprono funzioni di rappresentanza, amministrazione o direzione della Società;
b. coloro che esercitano, anche di fatto, la gestione ed il controllo della Società
c. coloro i quali operano nell'interesse della Società, cioè tutti i dipendenti di Amissima Holdings S.r.l. e delle società Controllate, indipendentemente dal un legame contrattuale o formale;
d. i Consulenti, i Fornitori, i procuratori e tutti coloro che operano per conto o nell'interesse della Società, in accordo con quanto contrattualmente previsto.

### 3.3 La costruzione del Modello e la sua struttura

La costruzione del Modello è stata preceduta da un'analisi preliminare, condotta dalla Società, considerando i contenuti del D. Lgs. 231/01, le indicazioni delle Politiche di Gruppo giudicate applicabili e le *best pratices* di mercato.

L'analisi ha avuto ad oggetto le seguenti attività:

- Individuazione delle aree "a rischio reato" e delle "attività sensibili" ovvero di quelle attività operative che nell'ambito delle aree a rischio possono, in linea teorica, comportare la commissione di uno o più reati tra quelli previsti dal Decreto (c.d. "Mappatura delle aree a rischio");
- disegno del Modello di organizzazione, gestione e controllo;
- predisposizione della documentazione costitutiva del Modello.

**Individuazione delle attività a rischio**

L'art. 6 comma 2 Lett. A del Decreto prevede espressamente che il Modello dell'ente individui le attività aziendali nel cui ambito possano essere potenzialmente commessi i reati dallo stesso previsti.
L'analisi è stata condotta dalla Società considerando il contesto organizzativo ed operativo di Amissima Holdings S.r.l. in relazione a tutte le fattispecie di reato previste dal D. Lgs. 231/01.
È stata a tal fine analizzata la documentazione aziendale pertinente (i.e. lo Statuto Sociale, il Sistema delle deleghe, il Manuale di Organizzazione, il Funzionigramma Aziendale Generale e relativo Organigramma, la normativa aziendale vigente, i contratti di accentramento delle funzioni di controllo, gli accordi di distacco del personale, il *Cost Sharing Agreement,* il contratto di *Cash Pooling* ecc. ) e sono stati tenuti in considerazione gli assetti di *governance*, i meccanismi di integrazione operativa con le società controllate ed i contenuti del Modelli di Organizzazione e Gestione ai sensi del D. Lgs. 231/01 adottati dalle controllate stesse.

All'esito dell'analisi:

- sono state individuate le Aree a rischio reato e le attività sensibili all'interno delle quali si possono potenzialmente verificare eventi pregiudizievoli per gli obiettivi del Decreto. Tale analisi è stata condotta tenendo conto sia delle attività direttamente svolte dalla Società, sia delle attività svolte per conto della Società dalle funzioni delle controllate;
- per ogni attività sensibile sono individuate le possibili modalità di realizzazione dei reati collegati;

- sono stati individuati c.d. *risk owners* ovvero i referenti, nell'ambito dell'organizzazione, responsabili delle aree a rischio reato.

**Disegno del Modello**

Nella seconda fase, in considerazione delle attività sensibili individuate, si è provveduto a rilevare le componenti del sistema di controllo esistente sia nella Società che nelle sue controllate e verificarne sia l'adeguatezza rispetto alle esigenze di prevenzione e controllo di cui al D. Lgs. 231/2001 sia la rispondenza rispetto all'effettiva operatività svolta.

Nell'ambito dell'analisi è stata posta particolare attenzione al riscontro dei seguenti principi di controllo che Amissima Holdings ritiene fondanti per un presidio efficace ed efficiente al rischio ex D. Lgs. 231/01:

Norme di comportamento

I codici etici e di comportamento devono descrivere le regole di condotta da seguire nello svolgimento di tutte le attività sensibili.

Definizione di ruoli e responsabilità

La documentazione organizzativa aziendale deve declinare ruoli e responsabilità delle unità organizzative a tutti i livelli descrivendo le attività proprie di ognuna di esse.
I ruoli e le responsabilità devono essere diffusi e conosciuti a tutti i livelli della struttura.

Protocolli e normativa aziendale

Le attività sensibili devono essere regolamentate in modo coerente attraverso gli strumenti normativi aziendali per poter individuare in ogni momento le modalità operative seguite, i controlli da attuare e le responsabilità attribuite.

Segregazione dei compiti

In ogni attività sensibile devono essere separate le funzioni ed i soggetti incaricati di assumere e/o eseguire una decisione ed i soggetti deputati ad elaborare l'evidenza contabile della stessa e a svolgere i controlli previsti dalla legge e dalle procedure e prassi aziendali.

Poteri autorizzativi e di firma

Esistenza di un sistema di deleghe che consenta la chiara identificazione di una specifica assegnazione di poteri e limiti ai soggetti che operano impegnando la Società e manifestandone la volontà,

L'attribuzione dei poteri deve essere coerente con le responsabilità organizzative assegnate e con l'idoneità tecnico-professionale del delegato.

Devono essere previsti meccanismi di pubblicità delle procure assegnate verso gli interlocutori esterni e meccanismi di rendicontazione dei poteri delegati.

Attività di controllo e tracciabilità delle operazioni

Nella normativa interna devono essere formalizzati i controlli operativi e le loro caratteristiche.

La documentazione afferente le attività sensibili deve essere adeguatamente formalizzata e archiviata in luogo idoneo alla conservazione, al fine di tutelare la riservatezza dei dati in essi contenuti e di evitare danni, deterioramenti e smarrimenti. L'accesso ai documenti archiviati deve essere sempre motivato e consentito solo alle persone autorizzate in base alle norme interne, al Collegio Sindacale o a funzioni e organi deputati al controllo compreso l'Organismo di Vigilanza.

La formazione degli atti e i relativi livelli autorizzativi, lo sviluppo delle operazioni deve essere adeguatamente formalizzata con evidenza della loro motivazione.

I controlli effettuati devono essere documentati e verificabili *ex-post* e ove opportuno, devono essere prodotti adeguati report di monitoraggio, che contengano evidenza dei controlli effettuati e di eventuali anomalie.

Flussi informativi

Esistenza di sistemi di flussi informativi che consentano di verificare il perseguimento di obiettivi strategici e il rispetto della normativa di monitorare e controllare il perseguimento degli obiettivi.

Sistema Sanzionatorio

Esistenza di adeguati sistemi sanzionatori per i destinatari del Modello (si rimanda al Capitolo 5).

Formazione e informazione

Adeguati processi di formazione, diffusione e comunicazione del Modello e sugli obblighi derivanti dal D. Lgs. 231/01 (si rimanda al Capitolo 1 Paragrafo 9).

## Impostazione della documentazione costitutiva del Modello di Organizzazione, Gestione e Controllo

Nella terza ed ultima fase è stata impostata la documentazione costitutiva del Modello di Organizzazione, Gestione e Controllo ex D. Lgs. 231/2001 della Società.

Il Modello è costituito secondo la seguente struttura:

1) **Parte generale**, nell'ambito della quale viene descritto il Modello nelle sue caratteristiche generali (finalità, destinatari, struttura e metodologia adottata, ruolo e funzionamento dell'Organismo di Vigilanza, informazione e diffusione del Modello ecc.) e il Sistema Disciplinare nel caso di mancata osservanza del Codice Etico e del MOG adottato ai sensi del D. Lgs. 231/2001;
2) **Parte speciale**, in cui vengono illustrate le aree di rischio e le attività sensibili individuate, le fattispecie di reato presupposto potenzialmente rilevanti per la Società (con relative esemplificazioni), le regole comportamentali, i principi ed i meccanismi di controllo previste per il presidio dei reati.

### 3.4 La procedura di adozione del Modello

Pur essendo l'adozione del Modello "facoltativa" ai sensi del D. Lgs. 231/01, Amissima Holdings ha deciso di dotarsi di un MOG, provvedendo all'approvazione del documento da parte del Consiglio di Amministrazione ed istituendo l'Organismo di Vigilanza.

Il Consiglio di Amministrazione è responsabile dell'aggiornamento del Modello e del suo adeguamento in relazione al mutamento degli assetti organizzativi, dei processi relativi nonché delle risultanze dei controlli. Per garantire che le variazioni del Modello siano operate con tempestività, il Consiglio di Amministrazione ha delegato all'Organismo di Vigilanza il compito di monitorare, con cadenza periodica, l'adeguatezza del Modello e quindi, richiedere alla Società, il relativo aggiornamento.

Le eventuali modifiche del Modello di carattere sostanziale, ossia dettate dall'evolversi della normativa di riferimento e/o da cambiamenti riguardanti i principi/fondamenti contenuti nel Modello, i poteri/doveri e la composizione dell'Organismo di Vigilanza, sono oggetto di approvazione da parte del Consiglio di Amministrazione.

Le modifiche diverse da quelle sostanziali sono valutate direttamente dall'OdV, il quale provvederà a comunicare al Consiglio di Amministrazione le modifiche effettuate, affinché provveda alla relativa ratifica.

### 3.5 Adozione del Modello da parte delle società controllate

Amissima Holdings intende garantire un complessivo efficacie presidio contro la commissione di reati all'interno del Gruppo; a tal fine la Holding promuove l'adozione e l'attuazione da parte di Amissima Vita S.p.A. e Amissima Assicurazioni S.p.A. di propri Modelli di Organizzazione e Gestione ai sensi del D. Lgs.231/01.

Nell'esercizio della rispettiva autonomia decisionale, Amissima Vita e Amissima Assicurazioni sono responsabili dell'adozione e attuazione dei propri Modelli rispondenti a quanto disposto dagli artt. 6 e 7 del Decreto.

L'adozione dei Modelli Organizzativi è deliberata dal Consiglio di Amministrazione di ogni Società.

Nell'adozione dei rispettivi Modelli, Amissima Vita e Amissima Assicurazioni tengono conto degli orientamenti forniti da Amissima Holdings nonché dei contenuti, della struttura e delle metodologie seguite per l'adozione del presente Modello.
Nel dare attuazione a tali indicazioni, le società controllate devono valutare autonomamente le specifiche aree di rischio in relazione alla attività da loro svolta, a seguito dell'analisi della propria struttura organizzativa e della propria operatività aziendale, tendendo comunque in considerazione i meccanismi di integrazione operativa con la Holding ed i contenuti del presente Modello.
Nell'adottare i propri modelli, Amissima Vita e Amissima Assicurazioni procedono alla nomina degli Organismi di Vigilanza delle società.

### 3.6 Coordinamento delle società del Gruppo per l'applicazione del D. Lgs. 231/01

Amissima Holdings promuove nel Gruppo il rispetto dei valori di correttezza e integrità che si declinano anche nella previsione di un complessivo sistema di presidio 231 adeguato ed efficace.
La funzione Normativa Aziendale di Amissima Holdings, con il supporto della Segreteria Societaria e dell'Ufficio Legale, ha il compito di garantire la coerenza dei Modelli 231 adottati dalle singole società del Gruppo nell'ambito delle rispettive responsabilità.
Ferma restando l'autonomia degli OdV di ciascuna Società del Gruppo, sono previsti momenti di incontro con cadenza periodica per discutere temi di interesse comune nella prospettiva di un costante miglioramento delle misure complessive connesse all'attuazione del D. Lgs.231/01.

Sono altresì previsti flussi informativi tra Amissima Holdings e le società del Gruppo, tramite i rispettivi OdV, nel caso di eventi rilevanti ai fini del D. Lgs.231/01, allo scopo di verificare la efficacia del sistema di presidio a livello di Gruppo e garantire la costante adeguatezza e coerenza dei rispettivi Modelli 231.

In coerenza con il proprio ruolo di direzione e coordinamento, Amissima Holdings, con l'adozione del presente Modello promuove:

- l'attivazione di flussi informativi aventi ad oggetto eventuali criticità e, più in generale, le esperienze maturate dalle singole società in relazione alla attuazione dei Modelli 231;
- meccanismi di coordinamento delle eventuali iniziative relative allo studio e all'approfondimento di tematiche afferenti il D. Lgs. 231/01, la loro interpretazione e applicazione all'interno del Gruppo al fine di garantire nel continuo la coerenza dei Modelli 231.

Gli OdV delle società del Gruppo ricevono adeguata informativa in merito allo stato e agli esiti degli adempimenti sopra descritti.

## 3.7 Informazione e diffusione del Modello

Amissima Holdings garantisce una corretta conoscenza e divulgazione delle regole di condotta contenute nel Modello nei confronti di tutti i portatori di interesse. In particolare, la Società provvede, anche tramite la pubblicazione sul sito Internet della Società e sugli applicativi informatici aziendali (Intranet aziendale), a portare conoscenza di tutti i destinatari (come da paragrafo 3.2) il presente Modello e il Codice Etico adottati dalla stessa e approvati dal Consiglio di Amministrazione.

### *3.7.1 Informazione ai Dipendenti*

Il livello di formazione ed informazione nei confronti dei dipendenti e dei portatori di interesse varia a seconda del ruolo e delle competenze degli stessi, con un diverso grado di approfondimento in relazione al differente coinvolgimento delle risorse nei processi sensibili ai sensi del D. Lgs. 231/2001.

L'attività informativa è seguita dalla Funzione Normativa Aziendale e si sostanzia nella pubblicazione sulla Intranet dei documenti che compongono il Modello, nonché delle sue regole di funzionamento (e.g. Codice Etico, Norme comportamentali, Normative interne aziendali, Codice Sanzionatorio); tale pubblicazione viene notificata a tutti i dipendenti e al personale

distaccato. La Società provvede altresì a consegnare la documentazione in questione anche ai soggetti neo assunti in fase di regolarizzazione del rapporto lavorativo.

Al fine di agevolare la comprensione dei principi a fondamento del Modello e di renderne più immediata ed efficace la diffusione, la Società organizza corsi formativi periodici volti all'approfondimento dei contenuti del Modello nonché, nel caso sia necessario, dell'evolversi della normativa di riferimento. L'attività formativa, rivolta a tutti i dipendenti e ai distaccati, si sostanzia in formazione frontale, con la partecipazione diretta in aula garantita dalla compilazione, da parte di ogni partecipante, di opportuni fogli firma (sia di entrata sia di uscita), oppure mediante lo svolgimento di moduli formativi in *e-learning*. In entrambi i casi, sono previsti dei test di valutazione (sia di entrata sia di uscita) al fine di poter verificare le conoscenze acquisite durante il corso.

L'attività di formazione è promossa e supervisionata dall'Organismo di Vigilanza, che si avvale del supporto operativo delle funzioni aziendali competenti e di consulenti esterni, pianificando **incontri periodici** in aula caratterizzati da specifici programmi di aggiornamento, cui viene associata un'**attività di formazione *e-learning* immediata** per le risorse neo assunte sia dalla Società che dalle controllate (in via definitiva o con rapporti di lavoro temporaneo).

Gli eventi formativi garantiscono l'aggiornamento sistematico del personale, cui vengono illustrate le ragioni giuridiche e di opportunità che ispirano le regole e la loro portata concreta; a tal riguardo, la Società valuta **interventi correttivi** a corredo della formazione periodica c.d. *standard* ogni qualvolta si verifichino comportamenti anomali che rivelino inottemperanza alle regole codificate o impongano revisioni e/o integrazioni dei protocolli operativi interni e comunque al termine di ciascun processo di *risk assessment*.

### *3.7.2 Informazione ai Collaboratori Esterni*

Per gli altri soggetti che collaborano a vario titolo con la Società, quest'ultima prevede, in fase di predisposizione del contratto, il trasferimento delle necessarie informazioni attestate con la sottoscrizione di specifiche clausole mediante le quali i soggetti in questione dichiarino di conoscere e rispettare principi e regole del Modello Organizzativo, nonché del Codice Etico adottato dalla Società.

# CAPITOLO 4 L'ORGANISMO DI VIGILANZA

## 4.1 Istituzione Dell'OdV

È istituito presso Amissima Holdings, in ottemperanza all'art. 6 del D. Lgs. 231/2001, l'Organismo di Vigilanza - a composizione collegiale mista - avente il compito di:

**a)** Vigilare sull'**effettività** del modello, verificando la coerenza tra i comportamenti concreti ed il modello istituito;

**b)** Valutare nel tempo l'**adeguatezza** del modello, ossia la sua reale (e non meramente formale) capacità di prevenire, in linea di massima, i comportamenti non voluti;

**c)** Curare il necessario **mantenimento e aggiornamento** in senso dinamico del modello, nell'ipotesi in cui le analisi operate rendano necessario effettuare correzioni ed adeguamenti;

**d)** Suggerire proposte di adeguamento e verificare l'attuazione e la effettiva funzionalità delle soluzioni proposte (c.d. ***follow-up***).

L'Organismo di Vigilanza è dotato di *autonomi poteri di iniziativa e controllo;* in particolare, i principali requisiti dell'Organismo sono:

- **Autonomia ed indipendenza**. L'Organismo di Vigilanza di Amissima Holdings, rispondendo solo al Consiglio di Amministrazione della Società, è collocato come unità di staff in una posizione assolutamente svincolata dalla linea gerarchica, con funzioni di informativa solo ai massimi livelli aziendali. All'OdV non sono attribuiti compiti operativi e poteri decisionali relativi all'attività della Società, che ne pregiudicherebbero la serenità di giudizio in sede di verifica, di controllo sui comportamenti adottati dai dipendenti e sulla tenuta del Modello. Le attività poste in essere dall'Organismo di Vigilanza non possono essere sindacate da alcun altro organismo o struttura aziendale, fermo restando che l'Organo Amministrativo è in ogni caso chiamato a svolgere un'attività di vigilanza sull'adeguatezza del suo intervento, in quanto all'organo amministrativo è ascrivibile la responsabilità ultima del funzionamento del Modello;

- **Professionalità**. L'Organismo di Vigilanza di Amissima Holdings possiede un bagaglio di strumenti e tecniche idoneo e adeguato per poter svolgere efficacemente l'attività assegnata. Tale requisito è altresì garantito dal fatto che l'Organismo stesso sia composto da membri dotati di specifiche competenze tecniche anche di natura ispettivo-consulenziale tra loro complementari;
- **Continuità di azione**. La connotazione dell'Organismo quale struttura dedicata esclusivamente all'attività di vigilanza sul Modello, priva di mansioni gestionali che la vincolino all'assunzione di decisioni con effetti economico-finanziari, garantisce il monitoraggio costante sulla concreta attuazione del Modello.

### 4.2 Nomina, composizione e regole di funzionamento dell'OdV

L'Organismo di Vigilanza di Amissima Holdings, nominato dal Consiglio di Amministrazione della Società, si compone da un minimo di tre fino ad un massimo di sette membri.

I membri dell'Organismo sono scelti tra soggetti particolarmente qualificati ed esperti nelle materie legali e nelle procedure di controllo ed in possesso dei requisiti di onorabilità previsti dal Decreto del Ministro dello Sviluppo Economico, n. 220/2001 Testo Unico delle leggi in materia Bancaria.

In un'ottica di razionalizzazione dei controlli e dei flussi informativi inerenti il monitoraggio del sistema di controllo aziendale, il Consiglio ha attribuito la funzione di Organismo di Vigilanza ex D. Lgs. 231/01 al Collegio Sindacale, coadiuvato dal Responsabile della Funzione di Internal Audit e da un esperto penalista esterno.

Ai componenti dell'Organismo, il Consiglio di Amministrazione conferisce più ampie facoltà e poteri per lo svolgimento delle attività contemplate nel modello.

I componenti dell'Organismo, salvo che non sia diversamente stabilito nella delibera di nomina, restano in carica per tre anni e sono rinnovabili. In ogni caso ciascun componente rimane in funzione fino alla nomina del successore.

Ove il Presidente o un componente dell'Organismo incorrano in una causa di incompatibilità (es. conflitto d'interesse), il Consiglio di Amministrazione, esperiti gli opportuni accertamenti e

sentito l'interessato, stabilisce un termine non inferiore a 30 giorni entro il quale deve cessare la situazione di incompatibilità. Trascorso tale termine senza che la predetta situazione sia cessata, il Consiglio di Amministrazione revoca il mandato. In ogni caso il componente che si trovi in una situazione di conflitto con la materia oggetto dell'attività o della decisione, deve astenersi dalla partecipazione alla stessa.

Il mandato sarà, altresì, revocato:

1) qualora sussistano circostanze tali da far venir meno i requisiti di autonomia e indipendenza richiesti dalla legge;
2) qualora vengano meno i requisiti di onorabilità di cui sopra;
3) nel caso di mancata partecipazione a più di tre riunioni consecutive senza giustificato motivo.

In caso di rinuncia, sopravvenuta incapacità, morte, revoca o decadenza di un membro effettivo dell'Organismo, gli altri componenti ne daranno comunicazione tempestiva al Consiglio di Amministrazione affinché provveda, ove necessario, a deliberare la nomina del sostituto.

In caso di rinuncia, sopravvenuta incapacità, morte, revoca o decadenza del Presidente, subentra a questi il membro effettivo più anziano (inteso come anzianità di carica nell'ODV), il quale rimane in carica fino alla data in cui il Consiglio di Amministrazione abbia deliberato la nomina del nuovo Presidente dell'Organismo.

La rinuncia da parte dei componenti dell'Organismo può essere esercitata in qualsiasi momento e deve essere comunicata al Consiglio di Amministrazione per iscritto unitamente alle motivazioni che l'hanno determinata. In caso di perdita dei requisiti di indipendenza ed autonomia, i membri dell'OdV comunicano la circostanza al Consiglio di Amministrazione il quale ne delibera la decadenza.

Il mandato deve essere revocato per giusta causa; per giusta causa di revoca dovrà intendersi:

a) l'interdizione o l'inabilitazione, ovvero una grave infermità che renda uno dei componenti dell'Organismo inidoneo a svolgere le proprie funzioni di vigilanza, o un'infermità che determini un pregiudizio/impedimento al regolare svolgimento delle attività demandate all'Organismo;
b) un grave inadempimento dei propri doveri così come definiti nel Modello di Organizzazione, Gestione e Controllo;

c) una sentenza di condanna della Società ai sensi del Decreto, passata in giudicato, ovvero un procedimento penale concluso tramite c.d. "patteggiamento", ove risulti dagli atti "l'omessa o insufficiente vigilanza" da parte dell'Organismo, secondo quanto previsto dall'art. 6, comma 1, lett. d) del Decreto.
d) una sentenza di condanna passata in giudicato, a carico di uno dei membri dell'Organismo per aver personalmente commesso uno dei reati previsti dal Decreto;
e) una sentenza di condanna passata in giudicato, a carico di uno dei componenti dell'Organismo ad una pena che importa l'interdizione, anche temporanea, dai pubblici uffici, ovvero l'interdizione temporanea dagli uffici direttivi delle persone giuridiche e delle imprese.

Nei casi sopra descritti, il Consiglio di Amministrazione provvede, ove necessario, a nominare il nuovo componente dell'Organismo in sostituzione di quello cui sia stato revocato il mandato. Qualora, invece, il potere di revoca venga esercitato, sempre per giusta causa, nei confronti di tutti i componenti dell'Organismo, il Consiglio di Amministrazione provvede a nominare un nuovo Organismo.

Nel caso in cui sia stata emessa una sentenza di condanna, il Consiglio di Amministrazione, nelle more del passaggio in giudicato della sentenza, disporrà la sospensione dei poteri dell'Organismo, o di uno dei suoi membri, e la nomina di un Organismo *ad interim*, o la nomina di un nuovo membro.

Qualora venisse meno, per sopravvenuta incapacità, morte, revoca, decadenza o dimissioni, la maggioranza dei membri dell'Organismo di Vigilanza, lo stesso decade automaticamente. In questo caso il Consiglio di Amministrazione provvede, entro 60 giorni, a nominare un nuovo Organismo di Vigilanza.

L'Organismo di Vigilanza si riunisce con cadenza almeno trimestrale, fatta salva la possibilità di riunirsi ogniqualvolta lo stesso ne ravvisi la necessità; le riunioni, documentate in appositi verbali sottoscritti da tutti i partecipanti, sono valide con la presenza della maggioranza dei membri in carica.

Nel caso in cui dovessero presentarsi eccezionali e temporanee situazioni di incompatibilità in relazione a specifiche attività di controllo, le stesse vengono superate con l'astensione da parte

del soggetto interessato; inoltre, in caso di parità tra voti favorevoli e contrari, si ritiene prevalente la decisione del Presidente.

I componenti dell'Organismo assicurano la riservatezza del segnalante in ordine alle informazioni di cui vengono in possesso – con particolare riferimento alle segnalazioni in ordine a presunte violazioni del Modello e dei suoi elementi costitutivi – e si astengono dal ricercare ed utilizzare informazioni riservate, per fini diversi da quelli indicati dall'art. 6 del D. Lgs. 231/01. In ogni caso, ogni informazione in possesso dei membri dell'Organismo è trattata in conformità con la legislazione vigente in materia e, in particolare, in conformità con il Codice in materia di protezione dei dati personali di cui al D. Lgs. 30 giugno 2003, n. 196.

### 4.3 Funzioni e poteri dell'OdV

L'Organismo di Vigilanza ha il compito di vigilare sull'osservanza del modello nonché sull'efficacia ed adeguatezza nel tempo dello stesso; in particolare, l'OdV svolge, con autonomi poteri, le seguenti attività:

a) promuovere la conoscenza e la comprensione del Modello nella Società;
b) vigilare sull'osservanza del Modello nella Società;
c) raccogliere, elaborare e conservare ogni informazione rilevante ai fini della verifica sull'osservanza del Modello;
d) vigilare sull'efficacia nel tempo del Modello, con particolare riferimento ai comportamenti riscontrati nel contesto della Società;
e) promuovere l'aggiornamento del Modello nell'ipotesi in cui si renda necessario e/o opportuno effettuare correzioni e adeguamenti dello stesso, in relazione alle mutate condizioni organizzative e/o legislative;
f) segnalare tempestivamente qualsiasi violazione del Modello ritenuta significativa, di cui sia venuto a conoscenza per segnalazione da parte dei dipendenti o dei portatori di interesse o che l'Organismo stesso abbia accertato. Le segnalazioni anonime saranno valutate discrezionalmente dall'Organismo, tenuto conto della gravità della violazione denunciata e delle indicazioni ivi contenute;

g) comunicare e relazionare su base continuativa al Consiglio di Amministrazione in ordine alle attività svolte, alle segnalazioni ricevute, agli interventi correttivi e migliorativi del Modello e al loro stato di realizzazione.

   Trasmettere, su base almeno semestrale, una **relazione informativa scritta** al Consiglio di Amministrazione (per le sue eventuali determinazioni e consequenziali articolazioni organizzative) riguardante:

   - le attività di verifica e controllo compiute nel corso dell'anno e l'esito delle stesse (anche con riferimento al programma originariamente elaborato);
   - i necessari e/o opportuni interventi correttivi e migliorativi del Modello e il loro stato di realizzazione;

h) promuovere la conoscenza dei principi contenuti nel Codice Etico e la loro traduzione in comportamenti coerenti da parte dei diversi destinatari individuando gli interventi formativi e di comunicazione più opportuni nell'ambito dei relativi piani annuali;

i) verificare e controllare periodicamente le aree/operazioni a rischio individuate nel Modello ed effettuare una ricognizione delle attività della Società con l'obiettivo di individuare le aree a rischio di reato e proporne l'aggiornamento e l'integrazione, ove se ne evidenzi la necessità;

j) istituire specifici canali informativi "dedicati", diretti a facilitare il flusso di segnalazioni ed informazioni verso l'Organismo;

k) segnalare al Consiglio di Amministrazione, sulla base dell'attività svolta, l'eventuale elaborazione o aggiornamento di protocolli, procedure operative e di controllo che regolamentino adeguatamente lo svolgimento delle attività, al fine di implementare il Modello.

l) vigilare sul costante svolgimento di programmi formativi, per quanto concerne l'evoluzione della normativa in argomento, rivolti sia al personale dipendente, sia ai distaccati, sia alla rete distributiva, anche collaborando con gli enti aziendali preposti per la relativa effettuazione;

m) segnalare la necessità di promuovere eventuali sanzioni disciplinari nel caso di accertate violazioni delle disposizioni di cui al Codice Etico ovvero del Modello;
n) documentare e conservare copia della documentazione inerente gli incontri con gli organi societari cui l'Organismo di Vigilanza riferisce, assicurando la tracciabilità delle attività svolte.

Per ottemperare alle proprie funzioni l'Organismo di Vigilanza attiva ed esegue indagini interne, avvalendosi del supporto della funzione di Internal Audit e/o di altre funzioni che, di volta in volta, si rendano a tal fine necessarie; inoltre, per poter adempiere ai compiti assegnatagli, l'Organismo di Vigilanza ha accesso ad ogni documento aziendale rilevante, senza necessità di alcun consenso preventivo.

L'Organismo di Vigilanza ha altresì la facoltà di relazionarsi con le funzioni aziendali deputate al controllo mediante un flusso informativo inerente sia i presidi delle aree di rischio individuate in relazione ai reati rilevanti ex D. Lgs. 231/01, sia la valutazione dell'efficacia e dell'efficienza del modello.

Per ogni esigenza necessaria al corretto svolgimento dei compiti ad esso assegnati, l'Organismo di Vigilanza potrà far affidamento su una adeguata dotazione di risorse finanziarie; il budget proposto annualmente dallo stesso OdV sarà approvato dall'Organo Amministrativo.

L'Organismo di Vigilanza può farsi assistere da consulenti esterni con competenze specialistiche e, laddove lo ritenga opportuno, ascoltare i consulenti della Società (in relazione agli incarichi di consulenza loro affidati).

### 4.4 Obblighi di informazione verso l'OdV

Ai sensi dell'art. 6, comma 1 lettera b) del D. Lgs 231/2001 all'Organismo di Vigilanza è affidato il compito di vigilare sul funzionamento e sull'osservanza del Modello di adottato dalla Società e di curarne l'aggiornamento.

A tal fine, l'articolo in commento stabilisce, al comma 2 lettera d), la necessità di prevedere specifici "*obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli*", ovvero, nei confronti dell'OdV.

Da ultimo, si evidenzia che la Legge 179/2017 è intervenuta sull'art. 6 del D. Lgs 231/2001 prescrivendo la previsione, all'interno del Modello di:

1. uno o più canali che consentano ai soggetti apicali e subordinati di presentare – a tutela dell'integrità dell'ente – segnalazioni circostanziate di condotte illecite (rilevanti ai sensi del D. Lgs. 231 e fondate su elementi di fatto precisi e concordanti) o di violazioni dello stesso Modello di Organizzazione e Gestione, di cui siano venuti a conoscenza in ragione delle funzioni svolte;
2. canali di segnalazione idonei a garantire la riservatezza dell'identità del segnalante nelle attività di gestione della segnalazione;
3. almeno un canale alternativo di segnalazione idoneo a garantire, con modalità informatiche, la riservatezza dell'identità del segnalante (c.d. *whistleblower)*;
4. un espresso divieto di atti di ritorsione o discriminatori (diretti o indiretti) nei confronti del segnalante (c.d. *whistleblower)*, per motivi collegati (direttamente o indirettamente) alla segnalazione;
5. apposite sanzioni nei confronti di chi viola le misure di tutela del segnalante, nonché di chi effettua con dolo o colpa grave segnalazioni che si rivelano infondate.

In considerazione di quanto sopra, la Società ha attivato i canali di seguito meglio specificati al fine di consentire, non solo ai soggetti apicali e subordinati, ma anche ai membri degli Organi Sociali, ai Fornitori e ai Collaboratori di presentare – a tutela dell'integrità dell'ente – segnalazioni circostanziate di condotte illecite (idonee a generare, anche solo in astratto, una eventuale responsabilità amministrativa della Società ai sensi del D. Lgs. 231/2001 e fondate su elementi di fatto precisi e concordanti) o di violazioni dello stesso Modello di Organizzazione e Gestione, di cui siano venuti a conoscenza in ragione delle funzioni e/o attività svolte. In particolare, le segnalazioni dovranno essere indirizzate per iscritto (in forma non anonima) all'Organismo di Vigilanza mediante una delle seguenti modalità:

**a)** inoltro mail all'indirizzo *OdV231-holding@amissima.it* (casella di posta elettronica gestita dall'Organismo di Vigilanza);

**b)** inoltro documenti a uno dei componenti dell'Organismo di Vigilanza;

**c)** comunicazione da indirizzarsi all'Organismo di Vigilanza presso la relativa Segreteria.

Gli obbligati dovranno comunicare all'OdV:

***i)*** le risultanze del controllo periodico effettuato in attuazione del modello (*report* riepilogativi dell'attività svolta, monitoraggi, indici consuntivi, ecc);

***ii)*** le anomalie o atipicità riscontrate nell'ambito dell'attività svolta e in considerazione delle informazioni disponibili (considerando che un fatto non rilevante, se singolarmente considerato, potrebbe assumere diversa valutazione in presenza di ripetitività o estensione dell'area di accadimento).

***iii)*** ogni notizia relativa alla possibile commissione di reati previsti dal Decreto acquisita direttamente e in ragione del rapporto di lavoro;

***iv)*** ogni altra segnalazione, anche di natura ufficiosa, relativa alla commissione, o alla ragionevole convinzione di commissione, dei Reati o comunque a comportamenti non in linea con le regole di condotta adottate dalla Società e dal Gruppo Amissima e che potrebbero ingenerare responsabilità ai sensi del Decreto.

Tali segnalazioni di condotte illecite, oltre che derivare da una conoscenza diretta del fatto nel corso del proprio lavoro, devono essere circostanziate e fondate su elementi di fatto precisi e concordanti. Non sono, pertanto, considerate le segnalazioni anonime, quelle non circostanziate e/o non fondate su elementi di fatto precisi e concordanti.

Tra le informazioni rilevanti possono essere in via esemplificativa indicate le seguenti:

a) le decisioni relative alla richiesta, erogazione ed utilizzo di finanziamenti pubblici;
b) le richieste di assistenza legale inoltrate dai dirigenti e/o dai dipendenti nei confronti dei quali la Magistratura procede per i reati previsti dalla richiamata normativa;
c) i provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i reati di cui al D. Lgs. n. 231/2001;
d) le commissioni di inchiesta o relazioni interne dalle quali emergano responsabilità per le ipotesi di reato di cui al D. Lgs. n. 231/2001;

e) le notizie relative alla effettiva attuazione, a tutti i livelli aziendali, del modello organizzativo, con evidenziazione dei procedimenti disciplinari attuabili con le relative valutazioni;
f) esiti di controlli – preventivi e successivi – e monitoraggio effettuati periodicamente[5] (inclusa la reportistica periodica in materia di salute e sicurezza sul lavoro).

Le segnalazioni verranno prese in considerazione e valutate dall'Organismo di Vigilanza i cui membri sono gli unici soggetti legittimati ad accedere alla casella di posta elettronica e, in generale, al contenuto delle segnalazioni allo stesso indirizzate. L'Organismo di Vigilanza garantisce la massima riservatezza nei confronti del segnalante, proteggendone l'identità.

L'Organismo di Vigilanza, valuta le segnalazioni ricevute e, ove necessario, si attiva tempestivamente e in modo efficace nelle attività indagine.
Si evidenzia che le informazioni fornite all'Organismo di Vigilanza mirano a consentire allo stesso di migliorare le proprie attività di pianificazione dei controlli e non, invece, ad imporgli attività di verifica puntuale e sistematica di tutti i fenomeni rappresentati; sull'Organismo, pertanto, non incombe un obbligo di agire ogni qualvolta vi sia una segnalazione, essendo rimesso alla sua discrezionalità e responsabilità stabilire in quali casi attivarsi.

Le attività di indagine e le eventuali successive azioni sono poste in essere in modo da preservare i segnalanti da qualsiasi forma di ritorsione, discriminazione o penalizzazione: in particolare, è fatto divieto di atti di ritorsione o discriminatori, diretti o indiretti, ivi incluso il mutamento di mansioni ai sensi dell'articolo 2103 del codice civile, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione.

L'adozione di misure discriminatorie nei confronti dei soggetti che effettuano le segnalazioni di cui sopra può essere denunciata all'Ispettorato nazionale del lavoro, per i provvedimenti di propria competenza.

[5] L'OdV riceve flussi periodici dalle funzioni di *Internal Audit, Risk Management, Compliance*, AML e Attuariale relativi alle relazioni periodiche effettuate sull'attività svolta nel periodo di riferimento.

La Società garantisce altresì la riservatezza dell'identità del segnalante, fatti salvi gli obblighi di legge e la tutela dei diritti della Società e delle persone accusate erroneamente o in mala fede. In particolare, fatte salve le richieste provenienti dall'autorità giudiziaria o dalle P.A. competenti, l'OdV e/o le funzioni aziendali deputate alla gestione della segnalazione: (i) possono rivelare l'identità del segnalante solo con il suo consenso o quando la conoscenza sia indispensabile per la difesa del segnalato, (ii) separano i dati identificativi del segnalante dal contenuto della segnalazione, in modo che la segnalazione possa essere processata in modalità anonima e rendere possibile la successiva associazione della segnalazione con l'identità del segnalante nei soli casi in cui ciò sia strettamente necessario.

Sono assicurati la riservatezza della procedura ed il diritto delle parti ad essere ascoltate dall'Organismo in merito alla segnalazione, prima che vengano assunte le specifiche determinazioni previste dal Codice Sanzionatorio.

# CAPITOLO 5 IL SISTEMA SANZIONATORIO

## 5.1 Funzione del sistema sanzionatorio

Il sistema sanzionatorio definisce le sanzioni previste per le infrazioni ai principi ed alle regole comportamentali sui quali si fonda il Modello. L'applicazione del sistema sanzionatorio presuppone la violazione delle disposizioni del Modello, pertanto la sanzione prescinde dall'integrazione di una specifica fattispecie di reato e viene comminata in caso di condotte poste in essere in violazione delle procedure codificate o disallineate rispetto ai protocolli definiti ai sensi del D. Lgs. 231/01, indipendentemente dallo svolgimento e dall'esito del procedimento penale eventualmente avviato dall'Autorità Giudiziaria.

Resta salva la facoltà per la Società di rivalersi per ogni danno e/o responsabilità che alla stessa possano derivare da comportamenti di Dipendenti, di Personale Distaccato e Collaboratori esterni in violazione del Modello Organizzativo.

I comportamenti sanzionabili che costituiscono violazione del Modello sono i seguenti:

- violazione delle procedure previste dal Modello o adozione, nell'espletamento delle attività sensibili, di comportamenti non conformi alle prescrizioni del Modello;
- violazione delle procedure previste dal Modello o adozione, nell'espletamento delle attività sensibili, di comportamenti palesemente in violazione delle prescrizioni del Modello stesso che espongano la Società ad una situazione oggettiva di rischio imminente di commissione di uno dei reati ex D. Lgs. 231/2001.

L'Organismo di Vigilanza, una volta ricevuta la segnalazione di infrazione, provvede, secondo le modalità previste dal Codice Sanzionatorio, a notificare l'accaduto al soggetto a cui l'infrazione è attribuita; provvede altresì a dare corso all'attività istruttoria al fine di verificare l'effettività e la gravità della violazione nonché la corretta individuazione del responsabile.

Al termine dell'istruttoria, l'Organismo di Vigilanza redige una relazione la quale viene trasmessa all'unità organizzativa preposta alla gestione del personale.

Le disposizioni che regolano la fase disciplinare si coniugano a quelle di rango superiore, ivi comprese quelle dei CCNL e delle leggi regolamentari, cui non possono derogare in nessun caso.

## 5.2 Il sistema sanzionatorio nei confronti dei Dipendenti soggetti al CCNL

La Società si è dotata di un Codice Sanzionatorio volto a disciplinare le violazioni, da parte di tutti i dipendenti (a qualsiasi titolo portatori di interessi), inclusi i dirigenti, alle disposizioni del Codice Etico e del Modello.

Per quanto riguarda l'accertamento delle violazioni e l'irrogazione della sanzione, la competenza è riservata di concerto all'Organismo di Vigilanza e all'Unità Organizzativa Responsabile della gestione del personale ai quali compete anche il monitoraggio del comportamento dei Dipendenti nella specifica prospettiva dell'osservanza del Modello.

L'applicazione delle sanzioni va graduata in ragione della violazione commessa; in tal senso, le sanzioni disciplinari per il personale dipendente tengono conto del principio di proporzionalità previsto dall'art. 2106 del Codice Civile, ossia della gravità oggettiva del fatto costituente l'infrazione disciplinare, il grado di colpa, l'eventuale reiterazione di un medesimo comportamento nonché l'intenzionalità del comportamento stesso.

In tal senso, coerentemente con le procedure previste dall'art. 7 della Legge del 20 maggio 1970 n. 300 (Statuto del Lavoratori) e con l'apparato sanzionatorio di cui al CCNL applicato da Amissima Holdings, i provvedimenti disciplinari irrogabili al personale dipendente sono i seguenti:

- **rimprovero verbale o biasimo scritto** per le mancanze lievi commesse per la prima volta ed esclusivamente qualificabili come colpose, ove esse non siano suscettibile di produrre effetti negativi verso l'esterno;
- **sospensione dal lavoro fino a 10 giorni** e **mancata retribuzione** per un importo non superiore a quattro ore della retribuzione base nel caso di infrazioni riguardanti obblighi di comunicazione o violazioni colpose lievi reiterate singolarmente passibili di richiamo verbale;
- **licenziamento** per comportamenti particolarmente gravi e/o ripetuti, determinati da una condotta colpevole del lavoratore che integri gravi violazioni del contratto o delle regole di diligenza e fedeltà previste dagli artt. 2104 e 2105 del Codice Civile, senza che possa distinguersi tra comportamenti che violino precetti penali di valore generale e quelli che infrangano regole della disciplina aziendale.

Le infrazioni agli obblighi di riservatezza, andranno valutate nella loro intrinseca essenza al fine di proporzionarne l'eventuale sanzione. Resta salva la circostanza che qualsivoglia comportamento doloso dovrà essere valutato con il massimo rigore.
Il contenuto del Codice Sanzionatorio, al pari del Codice Etico, è portato a conoscenza di tutti i dipendenti mediante la pubblicazione sugli applicativi informatici dedicati (Intranet aziendale).

### 5.3 Il Sistema sanzionatorio nei confronti dei Dirigenti

In caso di violazione del Modello da parte dei Dirigenti dei principi e delle regole di comportamento previste dal MOG e dal Codice Etico, la Società provvede ad applicare nei confronti dei responsabili la misura disciplinare più idonea fra quelle previste dal sistema sanzionatorio adottato.
Può costituire un illecito anche il mancato controllo, da parte del Dirigente, dei lavoratori gerarchicamente subordinati i quali hanno compiuto una violazione dei principi e delle regole di comportamento previste dal MOG e dal Codice Etico.

### 5.4 I provvedimenti relativi agli Amministratori

In caso di violazione del Modello da parte di uno o più membri del Consiglio di Amministrazione, l'Organismo di Vigilanza informa l'intero Organo Amministrativo i quali prendono gli opportuni provvedimenti.

### 5.5 I provvedimenti relativi ai Sindaci

In caso di violazione del Modello da parte di uno o più Sindaci, l'OdV informa il Consiglio di Amministrazione, i quali prendono gli opportuni provvedimenti tra cui, ad esempio, la convocazione dell'assemblea dei soci al fine di adottare le misure più idonee previste dalla legge.

### 5.6 I provvedimenti relativi ai Collaboratori Esterni

Ogni violazione alle regole del presente Modello commessa da collaboratori esterni è sanzionata secondo quanto previsto nelle specifiche clausole contrattuali inserite nei relativi contratti; le infrazioni possono comportare la risoluzione del rapporto contrattuale.

È fatto salvo il diritto di richiedere il risarcimento dei danno qualora dalla condotta di tali soggetti derivino danni alla Società, quali l'applicazione di una delle misure previste dal Decreto 231/2001.

### 5.7 I provvedimenti nei confronti dei membri dell'OdV

Ogni violazione alle regole del presente Modello commessa dai membri dell'OdV è segnalata dagli altri Membri, o dagli Amministratori all'intero Organo Amministrativo, il quale prende gli opportuni provvedimenti.

Risponde del reato di accesso abusivo ad un sistema informatico anche il soggetto che, pur essendo entrato legittimamente in un sistema, vi si sia trattenuto contro la volontà del titolare del sistema oppure il soggetto che abbia utilizzato il sistema per il perseguimento di finalità differenti da quelle per le quali era stato autorizzato.

***Esempio:***

Un dipendente neoassunto dalla Società accede abusivamente ai sistemi informatici della Società concorrente nella quale lavorava precedentemente al fine di copiare e, successivamente utilizzare dati ed informazioni commerciali di natura riservata.

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

La fattispecie di reato, ex art. 615 *quater* c.p., si realizza nel caso in cui, per procurare a sé o ad altri un profitto o arrecare ad altri un danno, abusivamente ci si procuri, si riproducano, si diffondano, si comunichino o si consegnino codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque si forniscano indicazioni o istruzioni idonee a tale scopo.

***Esempio:***

Un dipendente neoassunto dalla Società abusivamente diffonde le credenziali di accesso al sistema informatico di proprietà dell'impresa concorrente nella quale lavorava precedentemente, al fine di ottenere informazioni riservate.

Le ultime due fattispecie di reato sono trasversali alle attività sensibili individuate.

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

La fattispecie di reato, prevista all'art. 635 *bis* del c.p., si realizza nel caso in cui si distruggano, deteriorino o rendano, in tutto o in parte, inservibili sistemi informatici altrui, ovvero programmi, informazioni o dati altrui.

***Esempio:***

Un dipendente della Società procede alla cancellazione di un file contenente informazioni relative alla esistenza di un credito da parte di una delle controllate, senza essere stato preventivamente autorizzato da parte del responsabile del sistema.

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.)

La fattispecie di reato, delineata dall'art. 635 *ter* del c.p., si realizza nel caso in cui si commetta un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere sistemi informatici o telematici, informazioni, dati o programmi informatici utilizzati dallo Stato o da altro Ente pubblico o ad essi pertinenti, o comunque di pubblica utilità. Il reato è aggravato se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione dei sistemi informatici o telematici, delle informazioni, dei dati o dei programmi informatici.

***Esempio:***

Un dipendente della Società accede al sistema informatico dell'IVASS al fine di alterare o cancellare informazioni relative alla Società in esso contenute.

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

La fattispecie di reato, delineata dall'art.635 *quater* c.p., si realizza mediante le condotte di cui all'art.635 *bis* c.p. ovvero nel caso in cui attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, si distruggano, danneggino, rendano, in tutto o in parte, inservibili sistemi informatici o telematici altrui o se ne ostacoli gravemente il funzionamento.

Il reato si configura nel momento in cui l'alterazione dei dati ostacoli gravemente il funzionamento del sistema informatico.

Si veda, a titolo esemplificativo, l'esempio descritto in relazione all'art. 635 *bis.*

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

La fattispecie di reato, delineata dall'art.635 *quinquies* c.p., si realizza se il fatto di cui all'art.635 *quater* è diretto a distruggere, danneggiare, rendere, tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento.

L'elemento rilevante è che il sistema sia utilizzato per il perseguimento di pubblica utilità, indipendentemente dalla proprietà privata o pubblica del sistema stesso.

Si veda, a titolo esemplificativo, l'esempio descritto in relazione all'art. 635 *ter.*

Tali ultime fattispecie di reato sono trasversali a tutte le attività sensibili.

### 5.8 Le aree di rischio individuate

Le principali aree di rischio identificate sono le seguenti:

- Gestione IT
- Gestione risorse umane
- Amministrazione contabilità e bilancio
- Adempimenti societari.

Per un dettaglio delle attività sensibili connesse si rimanda all'Allegato 2 del Modello.

### 5.9 Regole di comportamento, procedure applicate e presidi di controllo

Al fine di prevenire e contrastare i reati informatici, è fatto divieto di:

- alterare documenti informatici, pubblici o privati, aventi efficacia probatoria;
- accedere abusivamente al sistema informatico o telematico di soggetti pubblici o privati;
- accedere abusivamente al proprio sistema informatico o telematico al fine alterare e /o cancellare dati e/o informazioni;
- detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso a un sistema informatico o telematico di soggetti concorrenti, pubblici o privati, al fine di acquisire informazioni riservate;

- detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso al proprio sistema informatico o telematico al fine di acquisire informazioni riservate;
- svolgere attività di approvvigionamento e/o produzione e/o diffusione di apparecchiature e/o software allo scopo di danneggiare un sistema informatico o telematico, di soggetti, pubblici o privati, le informazioni, i dati o i programmi in esso contenuti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento;
- svolgere attività fraudolenta di intercettazione, impedimento o interruzione di comunicazioni relative a un sistema informatico o telematico di soggetti, pubblici o privati, al fine di acquisire informazioni riservate;
- istallare apparecchiature per l'intercettazione, impedimento o interruzione di comunicazioni di soggetti pubblici o privati;
- svolgere attività di modifica e/o cancellazione di dati, informazioni o programmi di soggetti privati o soggetti pubblici o comunque di pubblica utilità;
- svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui;
- distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità.

Pertanto, i soggetti destinatari del presente Modello devono:

- utilizzare le informazioni, le applicazioni e le apparecchiature esclusivamente per motivi di ufficio;
- non prestare o cedere a terzi qualsiasi apparecchiatura informatica;
- custodire l'apparecchiatura hardware in dotazione con la diligenza, del c.d. "buon padre di famiglia";
- segnalare alle funzioni competenti il furto, il danneggiamento o lo smarrimento di tali strumenti; inoltre, qualora si verifichi un furto o si smarrisca un'apparecchiatura informatica di qualsiasi tipo, l'interessato, o chi ne ha avuto consegna, dovrà far pervenire alla funzione competente l'originale della denuncia all'Autorità di Pubblica Sicurezza;

- evitare di trasferire all'esterno della Società e/o trasmettere file, documenti, o qualsiasi altra documentazione riservata di proprietà della Società stessa o di altra Società del Gruppo, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni;
- evitare di lasciare accessibile ad altri il proprio Personal Computer (PC);
- evitare l'utilizzo di password di altri utenti aziendali, neanche per l'accesso ad aree protette in nome e per conto dello stesso;
- evitare l'utilizzo di strumenti software e/o hardware atti a intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
- utilizzare la connessione a Internet per gli scopi e il tempo strettamente necessario allo svolgimento delle attività che hanno reso necessario il collegamento;
- rispettare le procedure e gli standard previsti, segnalando senza ritardo alle funzioni competenti eventuali utilizzi e/o funzionamenti anomali delle risorse informatiche;
- installare e impiegare sulle apparecchiature della Società solo prodotti ufficialmente acquisiti dalla Società stessa;
- astenersi dall'effettuare copie non specificamente autorizzate di dati e di software;
- astenersi dall'utilizzare gli strumenti informatici a disposizione al di fuori delle prescritte autorizzazioni;
- osservare ogni altra norma specifica riguardante gli accessi ai sistemi e la protezione del patrimonio di dati e applicazioni della Società e del Gruppo;
- osservare scrupolosamente quanto previsto dalle politiche di sicurezza aziendali per la protezione e il controllo dei sistemi informatici.

Nell'ambito della gestione della sicurezza informatica, coerentemente con i principi di comportamento e di controllo generali, la regolamentazione dell'attività prevede:

- la definizione di apposite clausole nei rapporti contrattuali con società esterne, con cui i terzi dichiarino di conoscere e si obblighino a rispettare i principi contenuti nel Codice Etico e nel Modello della Società, nonché clausole risolutive espresse che attribuiscano alla Società la facoltà di risolvere i contratti in questione nel caso di violazione di tale obbligo;

- l'adozione di uno strumento normativo che assicuri la correttezza e la sicurezza dell'operatività dei sistemi informativi;
- strumenti per gestire la protezione delle informazioni contro accessi non autorizzati;
- la verifica dei log degli eventi concernenti la sicurezza.

Nell'ambito della gestione dei profili utente e del processo di autenticazione, coerentemente con i principi di comportamento e di controllo generali, la regolamentazione dell'attività prevede:

- il controllo degli accessi: il Gruppo ha adottato uno strumento normativo che disciplina gli accessi alle informazioni, ai sistemi informativi, alla rete, ai sistemi operativi, alle applicazioni. In particolare, tale strumento normativo prevede:
    - l'autenticazione individuale degli utenti tramite codice identificativo dell'utente e password o altro sistema di autenticazione sicura;
    - le liste di controllo del personale abilitato all'accesso ai sistemi, nonché le autorizzazioni specifiche dei diversi utenti o categorie di utenti;
    - una procedura di registrazione e destituzione per accordare e revocare l'accesso a tutti i sistemi e servizi informativi;
    - la rivisitazione dei diritti d'accesso degli utenti secondo intervalli di tempo prestabiliti usando un processo formale;
    - la destituzione dei diritti di accesso in caso di cessazione o cambiamento del tipo di rapporto che attribuiva il diritto di accesso;
    - l'accesso ai servizi di rete esclusivamente da parte degli utenti che sono stati specificatamente autorizzati e le restrizioni della capacità degli utenti di connettersi alla rete;
    - la chiusura di sessioni inattive dopo un predefinito periodo di tempo;
    - la custodia dei dispostivi di memorizzazione (ad es. chiavi USB, CD, hard disk esterni, etc.).
- la sicurezza nell'acquisizione, sviluppo e manutenzione dei sistemi informativi: lo strumento normativo definisce:

- controlli per l'implementazione di cambiamenti attraverso l'uso di formali procedure di *change management*;
- la gestione dei rischi di errori, perdite, modifiche non autorizzate di informazioni trattate dalle applicazioni;
- la disponibilità, l'integrità e la riservatezza delle informazioni;
- procedure per il controllo dell'installazione di software su sistemi.

Per quanto concerne la gestione e protezione delle reti (inclusa l'attività degli accessi da e verso l'esterno), la regolamentazione dell'attività prevede:

- la definizione di ruoli e le responsabilità nella gestione delle modalità di accesso di utenti esterni all'azienda e gli obblighi dei medesimi nell'utilizzo dei sistemi informatici, nonché nella gestione dei rapporti con i terzi in caso di accesso, gestione, comunicazione, fornitura di prodotti/servizi per l'elaborazione dei dati e informazioni da parte degli stessi terzi;
- adozione di uno strumento normativo per la gestione delle comunicazioni e dell'operatività, dello scambio di informazioni e dell'accesso alle reti;
- il controllo degli accessi alle informazioni, ai sistemi informativi, alla rete, ai sistemi operativi, alle applicazioni, verificando anche gli accessi da remoto.

Inoltre, la regolamentazione prevede:

- l'obbligo di restituzione dei beni forniti per lo svolgimento dell'attività lavorativa (ad es. personale computer, telefoni cellulari, token di autenticazione, etc.) per i dipendenti e i terzi al momento della conclusione del rapporto di lavoro e/o del contratto;
- la destituzione, per tutti i dipendenti e i terzi, dei diritti di accesso alle informazioni, ai sistemi e agli applicativi al momento della conclusione del rapporto di lavoro e/o del contratto o in caso di cambiamento della mansione svolta.

## 5.10 I controlli dell'Organismo di Vigilanza

L'Organismo di Vigilanza ha il potere di attivarsi con specifiche verifiche, anche a seguito di segnalazioni ricevute; l'Organismo ha altresì la facoltà di accedere a tutta la documentazione aziendale disponibile in materia, senza alcun obbligo di preavviso.

La Società ha altresì istituito, su richiesta dell'Organismo di Vigilanza, flussi informativi idonei a consentire a quest'ultimo di acquisire le informazioni utili per il monitoraggio periodico delle attività degli amministratori di sistema, della sicurezza dei sistemi informativi in considerazione di possibili intrusioni o incidenti rilevabili.

L'Organismo di Vigilanza, nell'espletamento delle attività di cui sopra, può avvalersi di tutte le risorse competenti in materia.