

**WELLCOMM ENGINEERING S.P.A.**

**MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO  
ai sensi del d.lgs. 231/2001**

## **Sommario**

### **PARTE GENERALE**

#### **1. DESCRIZIONE DEL QUADRO NORMATIVO**

- 1.1 *La responsabilità amministrativa*
- 1.2 *Fattispecie di reato*
- 1.3 *Autori del reato*
- 1.4 *Apparato sanzionatorio*
- 1.5 *Adozione del “modello di organizzazione e gestione” quale possibile esimente*

#### **2. ADOZIONE DEL MODELLO DA PARTE DI WELLCOMM**

- 2.1 *Obiettivi perseguiti da WELLCOMM con l'adozione del Modello*
- 2.2 *Reati rilevanti per WELLCOMM*
- 2.3 *Destinatari del Modello*
- 2.4 *Modifiche ed integrazioni del Modello*

#### **3. ORGANISMO DI VIGILANZA**

- 3.1 *Individuazione*
- 3.2 *Nomina*
- 3.3 *Funzioni e poteri dell'Organismo di Vigilanza*
- 3.4 *Reporting dell'Organismo di Vigilanza verso il vertice societario*
- 3.5 *Reporting verso l'Organismo di Vigilanza*
- 3.6 *Raccolta e conservazione delle informazioni*

#### **4. DIFFUSIONE, FORMAZIONE E COMUNICAZIONE**

- 4.1 *Diffusione*
- 4.2 *Piano di formazione e comunicazione*

#### **5. STRUTTURA DEL SISTEMA DISCIPLINARE**

- 5.1 *Funzione del sistema disciplinare*
- 5.2 *Violazione del Modello*
- 5.3 *Misure nei confronti del personale dipendente*
- 5.4 *Misure specifiche nei confronti dei Dirigenti*
- 5.5 *Misure nei confronti degli Amministratori*
- 5.6 *Misure nei confronti dei Sindaci*

## **PARTE SPECIALE**

### ***PARTE SPECIALE “A”***

#### ***I REATI CONTRO LA PUBBLICA AMMINISTRAZIONE***

- 1.A Potenziali aree a rischio*
- 2.A Principi di comportamento e controllo nelle principali aree di rischio*
- 3.A Principi per la prevenzione dei reati contro la Pubblica Amministrazione*

### ***PARTE SPECIALE “B”***

#### ***I REATI SOCIETARI***

- 1.B Potenziali aree a rischio*
- 2.B Principi di comportamento e controllo nelle principali aree di rischio*
- 3.B Principi per la prevenzione dei reati societari*

### ***PARTE SPECIALE “C”***

#### ***I REATI DI OMICIDIO COLPOSO E LESIONI COLPOSE GRAVI E GRAVISSIME, COMMESSI CON VIOLAZIONE DELLE NORME ANTINFORTUNISTICHE E SULLA TUTELA DELL’IGIENE E DELLA SALUTE SUL LAVORO***

- 1.C Potenziali aree a rischio*
- 2.C Principi di comportamento e controllo nelle principali aree di rischio*
- 3.C Principi per la prevenzione dei reati di omicidio colposo e lesioni colpose gravi e gravissime*

### ***PARTE SPECIALE “D”***

#### ***I REATI INFORMATICI***

- 1.D Potenziali aree a rischio*
- 2.D Principi di comportamento e controllo nelle principali aree di rischio*
- 3.D Principi per la prevenzione dei delitti informatici*

### ***ALLEGATI***

*Allegato 1 – Reati previsti dal d.lgs. 231/2001*

## **1. DESCRIZIONE DEL QUADRO NORMATIVO**

### **1.1 La responsabilità amministrativa**

Il decreto legislativo 8 giugno 2001 n. 231 (di seguito, “d.lgs 231/2001”) ha introdotto nell’ordinamento giuridico italiano la disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica (enti). Secondo tale disciplina le società possono essere ritenute responsabili, e conseguentemente sanzionate patrimonialmente, in relazione a taluni reati commessi o tentati *nell’interesse o a vantaggio della società* stessa dagli amministratori o dai dipendenti.

Il d.lgs 231/2001, allineandosi con i sistemi normativi di molti paesi europei, affianca alla responsabilità penale della persona fisica che ha commesso il reato l’autonoma responsabilità amministrativa dell’ente.

L’istituzione della responsabilità amministrativa della società nasce dalla considerazione che frequentemente le condotte illecite commesse all’interno dell’impresa non derivano da un’iniziativa privata del singolo, ma si ricollegano piuttosto a volontà e decisioni di vertice dell’ente medesimo.

### **1.2 Fattispecie di reato**

Le fattispecie di reato rilevanti ai sensi del d.lgs. 231/2001 sono quelle espressamente elencate dal legislatore - in ossequio al principio di legalità confermato dall’art. 2 del d.lgs. 231/2001 - e possono essere comprese nelle seguenti principali categorie:

- a) ***delitti contro la pubblica amministrazione*** (quali, indebita percezione di contributi e finanziamenti da parte dello Stato o di altro ente pubblico; truffa ai danni dello Stato e frode informatica ai danni dello Stato; corruzione per un atto d’ufficio o in atti giudiziari; concussione; malversazione a danno dello Stato o di altro ente pubblico);
- b) ***delitti contro la fede pubblica*** (quali falsità in monete, carte di pubblico credito e valori di bollo, indicati all’art. 25-bis d.lgs. 231/2001);
- c) ***reati societari*** (quali false comunicazioni sociali, falso in prospetto, falsità nelle relazioni o nelle comunicazioni della società di revisione; impedito controllo; illegale ripartizione degli utili e delle riserve; illecite operazioni sulle azioni o quote sociali; operazioni in pregiudizio dei creditori; formazione fittizia del capitale; illecita influenza sull’assemblea);
- d) ***delitti in materia di terrorismo e di eversione dell’ordine democratico*** (ivi incluso il finanziamento ai suddetti fini, indicati all’art. 25-quarter d.lgs. 231/2001);
- e) ***delitti contro la personalità individuale*** (quali lo sfruttamento della prostituzione, la pornografia minorile, indicati all’art. 25-quinquies d.lgs. 231/2001);

- f) *reati di lesioni colpose gravi e gravissime e omicidio colposo con violazione di norme antinfortunistiche.*
- g) *reati informatici*
- h) *delitti contro l'industria e il commercio*
- i) *delitti in materia di violazione del diritto d'autore*

Si rimanda all'Allegato 1 per l'elenco dettagliato dei reati di cui al d.lgs. 231/2001.

### **1.3 Autori del reato**

Quanto ai soggetti, il d.lgs. 231/2001 (art. 5) prevede la responsabilità dell'ente qualora il reato sia commesso:

- a) da *"persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo dell'ente stesso"* (c.d. soggetti in posizione apicale o "apicali"; art. 5, comma 1, lett. a), d.lgs. 231/2001);
- b) da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti in posizione apicale (c.d. soggetti sottoposti altrui direzione; art. 5, comma 1, lett. b), d.lgs. 231/2001).

La società non risponde, per espressa previsione legislativa (art. 5, comma 2, d.lgs. 231/2001), se le persone indicate hanno agito nell'interesse esclusivo proprio o di terzi.

### **1.4 Apparato sanzionatorio**

L'accertamento della responsabilità della società, attribuito al giudice penale, avviene (nell'ambito di un processo *ad hoc* nel quale l'ente viene parificato alla persona fisica imputata) mediante la verifica della sussistenza del reato presupposto per la responsabilità della società, nonché il sindacato di idoneità sui modelli organizzativi adottati.

Il d. lgs 231/2001 prevede un articolato sistema sanzionatorio. Le sanzioni possono essere:

- di **natura pecuniaria** (da Euro 25.000,00 fino ad un massimo di Euro 1.500.000,00 circa)
- di **natura interdittiva** (quali la sospensione o revoca di licenze e concessioni, il divieto di contrarre con la pubblica amministrazione, l'esclusione o revoca di finanziamenti e contributi), e
- **accessorie**: pubblicazione della sentenza e la confisca del prezzo o profitto del reato

Nelle ipotesi di commissione, nelle forme del tentativo, dei delitti indicati nel Capo 1 del d.lgs. 231/2001 (artt. da 24 a 25-*quinquies*), le sanzioni pecuniarie (in termini di importo) e le sanzioni interdittive (in termini di tempo) sono ridotte da un terzo alla metà, mentre è esclusa

l'irrogazione di sanzioni nei casi in cui l'ente impedisca volontariamente il compimento dell'azione o la realizzazione dell'evento (art. 26).

Secondo l'art. 4 del d.lgs. 231/2001, l'ente può essere chiamato a rispondere in Italia in relazione a reati - contemplati dallo stesso d.lgs. 231/2001 - commessi all'estero. La Relazione illustrativa del d.lgs. 231/2001 sottolinea, infatti, la necessità di non lasciare sfornita di sanzione una situazione criminologica di frequente verifica, anche al fine di evitare facili elusioni dell'intero impianto normativo in oggetto.

### ***1.5 L'adozione del "Modello di Organizzazione e di Gestione" quale possibile esimente***

Il d.lgs. 231/2001, nell'introdurre il suddetto regime di responsabilità amministrativa, prevede, tuttavia, una forma specifica di esonero da detta responsabilità qualora l'ente dimostri di aver adottato tutte le misure organizzative e gestionali idonee a prevenire la commissione di reati da parte di soggetti che operino per suo conto.

Il d.lgs. 231/2001 indica quali sono le componenti di un apparato organizzativo efficace ed effettivo (cosiddetto modello di organizzazione e gestione – il Modello) la cui corretta predisposizione porta ad escludere la responsabilità dell'ente.

Il Modello si può definire come un complesso organico di principi, regole, disposizioni, schemi organizzativi, funzionale alla realizzazione ed alla diligente gestione di un sistema di controllo e monitoraggio delle attività sensibili, al fine della prevenzione sulla commissione, anche tentata, dei reati previsti dal d.lgs. 231/2001. La finalità preventiva del Modello si esplica sia nei confronti di soggetti in posizione "apicale" che di soggetti sottoposti all'altrui direzione.

In particolare, il Modello deve:

- individuare le attività nel cui ambito possono essere commessi reati;
- prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni della società in relazione ai reati da prevenire;
- individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati;
- prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli;
- introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello;
- prevedere, in relazione alla natura ed alla dimensione dell'organizzazione, nonché del tipo di attività svolta, misure idonee a garantire lo svolgimento dell'attività nel rispetto della legge e a scoprire ed eliminare tempestivamente situazioni di rischio.

L'adozione di modelli organizzativi, astrattamente idonei a prevenire i reati di cui al d.lgs. 231/2001, deve essere corredata dall'efficace attuazione degli stessi e da una procedura che garantisca il tempestivo aggiornamento e adeguamento.

## **2. ADOZIONE DEL MODELLO DA PARTE DI WELLCOMM**

### **2.1 *Obiettivi perseguiti da WELLCOMM con l'adozione del Modello***

WELLCOMM ritiene conforme alle proprie politiche aziendali procedere all'attuazione del modello di organizzazione e gestione previsto dal d.lgs. 231/2001.

WELLCOMM ritiene, altresì, opportuno dotarsi di un Codice Etico, espressione dei valori e principi sui quali l'attività aziendale si ispira.

E' convinzione di WELLCOMM che l'adozione del Modello e del Codice Etico, pur non costituendo un obbligo di legge, rappresenti un passo fondamentale per indirizzare e sensibilizzare i comportamenti e le azioni di tutti coloro che agiscono in nome e per conto di WELLCOMM, affinché il loro operare sia sempre orientato al rispetto della legge e dei principi di correttezza e trasparenza.

Il Modello è ispirato alle Linee guida per la costruzione dei modelli di Organizzazione, Gestione e Controllo elaborate da Confindustria ed approvate il 31 marzo 2008 e successive modifiche.

Il Modello, unitamente al Codice Etico qui allegato, è stato adottato, all'unanimità, dal Consiglio di Amministrazione di WELLCOMM nel corso dell'adunanza del 4 Ottobre 2010

Con delibera del 4 Ottobre 2010 il Consiglio di Amministrazione di WELLCOMM ha nominato l'Organismo di Vigilanza.

### **2.2 *Reati rilevanti per WELLCOMM***

Ai sensi dell'art. 6 del d.lgs. 231/2001, che prevede che la società individui le attività nel cui ambito possono essere commessi i reati, WELLCOMM ha svolto un'analisi di tutte le attività aziendali, dei processi di formazione delle decisioni, nonché del sistema di controllo interno.

Tale analisi è stata condotta anche con il supporto di professionisti esterni, tramite l'analisi della documentazione aziendale interna rilevante e l'incontro con i responsabili delle singole aree di attività.

Sulla base dell'analisi di cui sopra e in considerazione della natura e dell'attività di WELLCOMM, ai fini del Modello sono considerati rilevanti unicamente i reati di cui agli artt. 24, 24 bis, 25, 25 bis.1, 25 ter, 25septies e 25 novies del d.lgs. 231/2001.

### **2.3 *Destinatari del Modello***

Sono destinatari del Modello tutti coloro che operano per il conseguimento dello scopo e degli obiettivi di WELLCOMM. Fra i destinatari del Modello è incluso tutto il personale di WELLCOMM; le disposizioni contenute nel Modello devono dunque essere rispettate dal personale dirigenziale che opera in nome e per conto di WELLCOMM e da tutti i dipendenti.

Gli altri destinatari del Modello sono i componenti degli organi sociali di WELLCOMM, gli agenti, i rappresentanti commerciali, i procacciatori d'affari ed ogni collaboratore/consulente esterno, soggetti terzi, con i quali WELLCOMM opera (di seguito, congiuntamente, i "Destinatari").

### **2.4 *Modifiche ed integrazioni del Modello***

Il Modello è espressione della politica aziendale perseguita dai massimi vertici sociali. Pertanto, il potere di integrare e/o modificare il Modello è demandato al Consiglio di Amministrazione di WELLCOMM.

## **3. ORGANISMO DI VIGILANZA**

### **3.1 *Individuazione***

L'Organismo di Vigilanza è costituito in forma collegiale ed è composto da 2 membri, nominati con delibera del Consiglio di Amministrazione di WELLCOMM del 4 Ottobre 2010.

L'Organismo di Vigilanza definisce e svolge le attività di competenza ed è dotato, ai sensi dell'art. 6, comma 1, lett. b), del d.lgs. 231/2001, di "*autonomi poteri di iniziativa e controllo*".

Al fine di coadiuvare la definizione e lo svolgimento delle attività di competenza e di consentire la massima adesione ai requisiti e ai compiti di legge, l'Organismo di Vigilanza è autorizzato ad avvalersi di consulenti esterni specializzati.

Per il corretto e regolare esercizio delle sue funzioni, l'Organismo di Vigilanza potrà disporre di proprie risorse finanziarie che, su proposta dello stesso, gli saranno accordate dal Consiglio di Amministrazione di WELLCOMM, sentito il Collegio Sindacale.

Il Consiglio di Amministrazione, sentito il Collegio Sindacale, potrà riconoscere emolumenti all'Organismo di Vigilanza, da stabilirsi nell'atto di nomina o con successiva delibera.

### **3.2 Nomina**

L'Organismo di Vigilanza è istituito con delibera del Consiglio di Amministrazione di WELLCOMM, sentito il parere del Collegio Sindacale.

Costituiscono cause di ineleggibilità e/o di decadenza dell'Organismo di Vigilanza e della risorsa umana dedicata:

- la condanna, con sentenza passata in giudicato, per aver commesso uno dei reati previsti dal d.lgs. 231/2001; ovvero
- la condanna, con sentenza passata in giudicato, a una pena che comporta l'interdizione, anche temporanea, dai pubblici uffici, ovvero l'interdizione temporanea dagli uffici direttivi delle persone giuridiche e delle imprese.

In casi di particolare gravità, anche prima del giudicato, il Consiglio di Amministrazione di WELLCOMM potrà disporre - sentito il parere del Collegio Sindacale - la sospensione dei poteri dell'Organismo di Vigilanza e la nomina di un *interim*.

Fatta salva l'ipotesi di una rivisitazione del ruolo e del posizionamento dell'Organismo di Vigilanza sulla base dell'esperienza di attuazione del Modello, l'eventuale revoca degli specifici poteri propri dell'Organismo di Vigilanza potrà avvenire soltanto per giusta causa, previa delibera del Consiglio di Amministrazione di WELLCOMM sentito il parere del Collegio Sindacale.

### **3.3 Funzioni e poteri dell'Organismo di Vigilanza**

I compiti dell'Organismo di Vigilanza sono così definiti:

- vigilanza sull'effettività del Modello;
- disamina dell'adeguatezza del Modello, ossia dell'efficacia nel prevenire i comportamenti illeciti;
- analisi circa il mantenimento, nel tempo, dei requisiti di solidità e funzionalità del Modello;
- promozione dell'aggiornamento ed adeguamento continuo del Modello e del sistema di vigilanza sull'attuazione dello stesso;
- assicurazione dei flussi informativi di competenza.

Nello svolgimento dei compiti assegnati, l'Organismo di Vigilanza ha accesso senza limitazioni alle informazioni aziendali per le attività di indagine, analisi e controllo. E' fatto obbligo di informazione all'Organismo di Vigilanza, in capo a qualunque funzione aziendale, dipendente e/o componente degli organi sociali di WELLCOMM, a fronte di richieste da parte dell'Organismo di Vigilanza o al verificarsi di eventi o circostanze rilevanti.

### **3.4 Reporting dell'Organismo di Vigilanza verso il vertice societario**

L'Organismo di Vigilanza riferisce in merito all'attuazione del Modello, all'emersione di eventuali aspetti critici e comunica l'esito delle attività svolte nell'esercizio dei compiti assegnati. Sono previste le linee di riporto seguenti:

- continuativa, nei confronti del Presidente e dell'Amministratore Delegato di WELLCOMM, i quali informano il Consiglio di Amministrazione di WELLCOMM;
- semestrale, nei confronti del Collegio Sindacale di WELLCOMM, predisponendo un rapporto semestrale relativo all'attività svolta ed a eventuali innovazioni legislative in materia.

In particolare, alla notizia di una violazione del Modello commessa da parte di uno o più membri del Consiglio di Amministrazione, l'Organismo di Vigilanza informa il Consiglio di Amministrazione ed il Collegio Sindacale. Il Consiglio di Amministrazione procede agli accertamenti necessari e assume, sentito il Collegio Sindacale, i provvedimenti opportuni.

Alla notizia di una violazione del Modello commessa da parte di uno o più Sindaci, l'Organismo di Vigilanza informa il Consiglio di Amministrazione ed il Collegio Sindacale. Il Collegio Sindacale procede agli accertamenti necessari e assume, sentito il Consiglio di Amministrazione, i provvedimenti opportuni.

### **3.5 Reporting verso l'Organismo di Vigilanza**

L'Organismo di Vigilanza deve essere informato, mediante apposite segnalazioni da parte dei soggetti tenuti all'osservanza del Modello, in merito a eventi che potrebbero ingenerare responsabilità della Società ai sensi del d.lgs. 231/2001. Valgono al riguardo le seguenti prescrizioni di carattere generale:

- devono essere raccolte da ciascun responsabile di Divisione della Società eventuali segnalazioni relative alla commissione, o al ragionevole pericolo di commissione, dei reati contemplati dal d.lgs. 231/2001 o comunque a comportamenti in generale non in linea con le regole di comportamento di cui al Modello e al Codice Etico;
- ciascun dipendente deve segnalare la violazione (o presunta violazione) del Modello contattando il proprio diretto superiore gerarchico e/o l'Organismo di Vigilanza;
- i consulenti, i collaboratori e i partner commerciali, per quanto riguarda la loro attività svolta nei confronti della Società, effettuano la segnalazione direttamente all'Organismo di Vigilanza;
- l'Organismo di Vigilanza valuta le segnalazioni ricevute e le attività da porre in essere; gli eventuali provvedimenti conseguenti sono definiti e applicati in conformità a quanto *infra* previsto in ordine al sistema disciplinare.

I soggetti che effettuano le segnalazioni in buona fede sono garantiti contro qualsiasi forma di ritorsione, discriminazione o penalizzazione e, in ogni caso, sarà assicurata la

riservatezza dell'identità del segnalante, fatti salvi gli obblighi di legge e la tutela dei diritti della Società o delle persone accusate in mala fede.

Oltre alle segnalazioni relative a violazioni di carattere generale sopra descritte, devono essere trasmesse all'Organismo di Vigilanza le notizie relative ai procedimenti disciplinari azionati in relazione alla violazione del Modello e del Codice Etico e alle sanzioni irrogate ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni.

### **3.6 *Raccolta e conservazione delle informazioni***

Ogni informazione, segnalazione, *report* previsti nel Modello sono conservati dall'Organismo di Vigilanza in un apposito *data base* informatico e/o cartaceo. I dati e le informazione così archiviate sono poste a disposizione di soggetti esterni all'Organismo di Vigilanza previa autorizzazione dell'Organismo di Vigilanza stesso.

## **4. FORMAZIONE E COMUNICAZIONE**

### **4.1 *Diffusione***

E' data ampia diffusione, all'interno ed all'esterno della struttura, dei principi contenuti nel Modello e del Codice Etico.

WELLCOMM si impegna a facilitare e promuovere la conoscenza del Modello e del Codice Etico da parte dei dipendenti, con grado di approfondimento diversificato a seconda della posizione e del ruolo, e il loro contributo costruttivo sui suoi contenuti.

### **4.2 *Piano di formazione e comunicazione***

Il Modello ed il Codice Etico sono comunicati formalmente dall'Organismo di Vigilanza a ciascun componente degli organi sociali, che li sottoscrive per adesione.

I principi e i contenuti del Modello e del Codice Etico sono comunicati formalmente dall'Organismo di Vigilanza a tutti i dirigenti della Società e ai Responsabili di Divisione, mediante consegna del presente documento.

I principi e i contenuti del Modello e del Codice Etico sono, inoltre, divulgati mediante corsi di formazione ai quali i soggetti sopra individuati sono tenuti a partecipare. La struttura dei corsi di formazione è definita dall'Organismo di Vigilanza in coordinamento con le funzioni aziendali competenti.

Il Modello e il Codice Etico sono affissi nelle bacheche aziendali e i principi e i contenuti del Modello e del Codice Etico sono comunicati a ciascun dipendente.

Il Modello e il Codice Etico sono portati a conoscenza di coloro con i quali WELLCOMM intrattiene relazioni d'affari.

## **5. STRUTTURA DEL SISTEMA DISCIPLINARE**

### **5.1 *Funzione del sistema disciplinare***

L'art. 6, comma 2, lett. e) e l'art. 7, comma 4, lett. b) del d.lgs. 231/2001 stabiliscono (con riferimento sia ai soggetti in posizione apicale sia ai soggetti sottoposti ad altrui direzione) la necessaria predisposizione di un “*sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello*”.

La definizione di sanzioni, commisurate alla violazione, applicabili in caso di violazione delle misure contenute nel Modello ha lo scopo di contribuire all'efficacia del Modello stesso ed all'efficacia dell'azione di controllo dell'Organismo di Vigilanza.

L'applicazione del sistema è autonoma rispetto allo svolgimento e all'esito del procedimento penale eventualmente avviato presso l'Autorità giudiziaria competente.

### **5.2 *Violazione del Modello***

Ai fini dell'ottemperanza del d.lgs. 231/2001, a titolo esemplificativo, costituisce violazione del Modello:

- la messa in atto di azioni o comportamenti non conformi alle prescrizioni del Modello, ovvero l'omissione di azioni o comportamenti prescritti dal Modello, nell'espletamento di attività nel cui ambito ricorre il rischio di commissione dei reati contemplati dal d.lgs. 231/2001;
- la messa in atto di azioni o comportamenti non conformi alle prescrizioni del Modello, ovvero l'omissione di azioni e comportamenti prescritti dal Modello, che:
  - (a) esponano la Società a una situazione oggettiva di rischio di commissione di uno dei reati contemplati dal d.lgs. 231/2001; e/o
  - (b) siano diretti in modo univoco al compimento di uno o più reati contemplati dal d.lgs. 231/2001; e/o
  - (c) tali da determinare l'applicazione a carico della società di sanzioni previste dal d.lgs. 231/2001;
- la messa in atto di azioni o comportamenti non conformi ai principi contenuti nel Codice Etico, ovvero l'omissione di azioni o comportamenti prescritti dal Codice Etico.

### **5.3 *Misure nei confronti del personale dipendente.***

Alla notizia di una violazione del Modello comunicata da parte dell'Organismo di Vigilanza, corrisponde l'avvio della procedura di accertamento delle mancanze stabilite dal Contratto Collettivo Nazionale del Lavoro per i Metalmeccanici – Industria CCNL. Pertanto:

- a ogni notizia di violazione del Modello comunicata da parte dell'Organismo di Vigilanza, è dato impulso da parte del Presidente e/o dell'Amministratore Delegato di WELLCOMM alla procedura di accertamento;

- nel caso in cui, a seguito della procedura, sia accertata la violazione del Modello, è individuata dal Presidente e/o dall'Amministratore Delegato di WELLCOMM, di intesa con il Responsabile delle Risorse Umane e da quest'ultimo irrogata nei confronti dell'autore della condotta censurata, la sanzione disciplinare prevista dal CCNL;
- la sanzione irrogata è proporzionata alla gravità della violazione.

Le sanzioni disciplinari previste dal CCNL sono:

- rimprovero verbale;
- rimprovero scritto;
- multa;
- sospensione dal lavoro e dalla retribuzione;
- licenziamento per giusta causa.

Il Responsabile delle Risorse Umane comunica l'irrogazione di tale sanzione all'Organismo di Vigilanza.

#### **5.4 Misure specifiche nei confronti di Dirigenti.**

Alla notizia di una violazione del Modello comunicata da parte dell'Organismo di Vigilanza, nel caso in cui la violazione del Modello da parte di uno o più dirigenti sia accertata ai sensi del precedente paragrafo 5.3, WELLCOMM adotterà nei confronti dell'autore della condotta censurata quanto previsto per legge e per CCNL. Se la violazione del Modello fa venire meno il rapporto di fiducia, la sanzione è individuata nel licenziamento per giusta causa.

#### **5.5 Misure nei confronti degli Amministratori**

L'Organismo di Vigilanza informa il Collegio Sindacale e tutti gli Amministratori della notizia di una violazione del Modello commessa da parte di uno o più membri del Consiglio di Amministrazione di WELLCOMM. Il Consiglio di Amministrazione di WELLCOMM procede agli accertamenti necessari e assume, sentito il Collegio Sindacale, i provvedimenti opportuni.

#### **5.6 Misure nei confronti dei Sindaci**

L'Organismo di Vigilanza informa tutti i Sindaci e il Consiglio di Amministrazione di WELLCOMM della notizia di una violazione del Modello commessa da parte di uno o più sindaci. Il Collegio Sindacale procede agli accertamenti necessari e assume, sentito il Consiglio di Amministrazione, i provvedimenti opportuni.

## PARTE SPECIALE “A”

### *I REATI CONTRO LA PUBBLICA AMMINISTRAZIONE*

In questa *parte speciale* sono individuate le aree di attività nel cui ambito possono essere commessi i reati di cui al d.lgs. 231/2001 che riguardano i rapporti con la Pubblica Amministrazione, così come identificati nell’Allegato 1).

#### **1.A Potenziali aree a rischio**

In considerazione delle attività svolte dalla Società e della struttura interna adottata, ai sensi dell’art. 6 del d.lgs. 231/2001, sono individuate le seguenti categorie di operazioni ed attività a rischio, nelle quali potrebbero essere commessi i reati previsti dagli artt. 24 e 25 del d.lgs. 231/2001:

- a) la partecipazione a procedure per l’ottenimento di erogazioni, contributi o finanziamenti da parte di organismi pubblici italiani o comunitari ed il loro concreto impiego;
- b) la gestione dei rapporti con soggetti pubblici per l’ottenimento di autorizzazioni e licenze per l’esercizio delle attività aziendali;
- c) la gestione dei rapporti con i soggetti pubblici per gli aspetti che riguardano la sicurezza e l’igiene sul lavoro;
- d) la gestione dei rapporti con i soggetti pubblici relativi all’assunzione di personale appartenente a categorie protette o la cui assunzione è agevolata;
- e) la gestione di trattamenti previdenziali del personale e/o gestione dei relativi accertamenti/ispezioni;
- f) la richiesta di provvedimenti amministrativi occasionali/*ad hoc* necessari allo svolgimento di attività strumentali a quelle tipiche aziendali;
- g) la gestione di beni mobili registrati legati all’attività aziendale;
- h) la predisposizione di dichiarazioni dei redditi o dei sostituti di imposta o di altre dichiarazioni funzionali alla liquidazione di tributi in genere;
- i) gli adempimenti presso soggetti pubblici, quali comunicazioni, dichiarazioni, deposito atti e documenti, pratiche, ecc. differenti da quelli descritti ai precedenti punti e nelle verifiche/accertamenti/procedimenti sanzionatori che ne derivano;
- j) la gestione di procedimenti giudiziari, arbitrari e/o di conciliazione;
- k) la gestione dei rapporti con le Autorità Pubbliche di Vigilanza.

Eventuali integrazioni delle suddette aree di attività a rischio potranno essere disposte dall’Organismo di Vigilanza al quale è dato mandato di individuare le relative ipotesi

## **2.A Principi di comportamento e controllo nelle principali aree di rischio**

E' vietato porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (artt. 24 e 25 del d.lgs. 231/2001). Sono altresì proibite le violazioni dei principi e delle procedure aziendali previste nella presente Parte Speciale.

Al fine di evitare il perfezionamento di reati nei confronti della Pubblica Amministrazione, tutti i Destinatari devono attenersi alle seguenti condotte:

- a) osservare rigorosamente tutte le leggi, i regolamenti e le procedure che disciplinano i rapporti e/o i contatti della Società con la Pubblica Amministrazione;
- b) improntare i rapporti con la Pubblica Amministrazione alla massima trasparenza, correttezza ed imparzialità;
- c) verificare, mediante il controllo esercitato dai responsabili delle diverse aree, che qualsiasi rapporto con la Pubblica Amministrazione sia svolto in modo lecito e regolare;
- d) evitare qualsiasi possibile situazione di conflitto di interessi con la Pubblica Amministrazione.

In conformità a tali principi è fatto pertanto divieto di:

- a) usare la propria posizione per ottenere benefici o privilegi per sé o per altri;
- b) effettuare o acconsentire ad elargizioni o promesse di denaro, beni o altre utilità di qualsiasi genere ad esponenti della Pubblica Amministrazione o a soggetti terzi da questi indicati o che abbiano con questi rapporti diretti o indiretti di qualsiasi natura;
- c) distribuire omaggi, regali o prestazioni di qualsiasi natura al di fuori di quanto previsto dalle procedure aziendali (vale a dire, ogni forma di regalo offerto o ricevuto, eccedente le normali pratiche commerciali o di cortesia, o comunque rivolto ad acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale). In particolare, è vietata qualsiasi forma di regalo a funzionari pubblici italiani ed esteri o a loro familiari che possa influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per l'azienda. Gli omaggi consentiti si caratterizzano sempre per l'esiguità del loro valore;
- d) accordare altri vantaggi di qualsiasi natura (promesse di assunzione ecc.) in favore di rappresentanti della Pubblica Amministrazione che possano determinare le stesse conseguenze sopra previste;
- e) riconoscere compensi in favore dei collaboratori esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere e alle prassi vigenti in ambito locale;

- f) presentare dichiarazioni non veritiere o incomplete, o comunque indurre in errore, organismi pubblici nazionali o comunitari al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati;
- g) porre in essere artifici e/o raggiri, tali da indurre in errore e da arrecare un danno allo Stato o ad altro ente pubblico o all'Unione Europea o ad organismi di diritto pubblico internazionale per realizzare un ingiusto profitto;
- h) promettere e/o versare somme, beni in natura e/o altri benefici nei rapporti con i rappresentanti delle forze politiche e/o di associazioni portatrici di interessi, per promuovere o favorire interessi della Società, anche a seguito di illecite pressioni;
- i) destinare somme ricevute da organismi pubblici nazionali o comunitari a titolo di erogazioni, contributi o finanziamenti per scopi diversi da quelli cui erano destinati;
- j) accedere senza autorizzazione ai sistemi informatici della Pubblica Amministrazione per ottenere e/o modificare informazioni nell'interesse o a vantaggio della Società.

### **3.A *Principi per la prevenzione dei reati contro la Pubblica Amministrazione***

Per le attività nell'ambito delle categorie di operazioni a rischio sopra individuate, sono previste specifiche procedure; in particolare:

- a) i rapporti nei confronti della Pubblica Amministrazione, per le suddette aree di attività a rischio, devono essere gestiti in modo unitario, procedendo alla nomina di un apposito responsabile per ogni operazione o pluralità di operazioni (in caso di particolare ripetitività delle stesse) svolte nelle aree di attività a rischio;
- b) di ogni operazione a rischio occorre dare debita evidenza per iscritto in modo che siano ricostruibili la formazione degli atti e i relativi livelli autorizzativi, a garanzia della trasparenza delle scelte effettuate;
- c) non vi deve essere identità soggettiva fra coloro che assumono o attuano le decisioni, coloro che devono dare evidenza contabile delle operazioni decise e coloro che sono tenuti a svolgere sulle stesse operazioni i controlli previsti dalla legge e dalle procedure contemplate dal sistema di controllo interno;
- d) i documenti riguardanti l'attività d'impresa devono essere archiviati e conservati, a cura della funzione competente, in conformità alla normativa sulla privacy ed al relativo regolamento aziendale sulla privacy adottato da WELLCOMM in data 27 marzo 2010;
- e) nessuno tipo di pagamento può essere effettuato in contanti o in natura, salva specifica preventiva autorizzazione da parte della funzione Amministrazione Finanza e Controllo per le operazioni di cassa di importo inferiore a *Euro 2.500,00 (duemilacinquecento)*;
- f) la scelta di consulenti esterni deve essere motivata ed avvenire sulla base di requisiti di professionalità, indipendenza, competenza e congruità dei costi;

- g) non devono essere corrisposti compensi, provvigioni o commissioni ad agenti, partners commerciali, collaboratori e/o fornitori in misura non congrua rispetto alle prestazioni rese alla Società e/o comunque non conformi all'incarico conferito, da valutare in base a criteri di ragionevolezza e in riferimento alle condizioni o prassi esistenti sul mercato o determinate da tariffe;
- h) i sistemi di remunerazione premianti i dipendenti e collaboratori devono rispondere a obiettivi realistici, misurabili, motivati e coerenti con le mansioni e l'attività svolta e con le responsabilità affidate;
- i) i contratti con collaboratori, agenti, distributori e fornitori devono contenere clausole e condizioni che richiamino alla conoscenza e al rispetto del d.lgs 231/2001 e del Codice Etico di WELLCOMM;
- j) le dichiarazioni rese a organismi pubblici nazionali o comunitari ai fini dell'ottenimento di erogazioni, contributi o finanziamenti, devono contenere solo elementi assolutamente veritieri e, in caso di ottenimento degli stessi, deve essere effettuato, ove previsto, apposito rendiconto;
- k) coloro che svolgono una funzione di controllo e supervisione su adempimenti connessi all'espletamento delle suddette attività devono riferire immediatamente all'Organismo di Vigilanza eventuali situazioni di irregolarità.

L'Organismo di Vigilanza propone le modifiche e le eventuali integrazioni delle prescrizioni di cui sopra e delle relative procedure di attuazione.

## PARTE SPECIALE “B”

### *I REATI SOCIETARI*

In questa *parte speciale* sono individuate le aree di attività nel cui ambito possono essere commessi i reati societari di cui al d.lgs. 231/2001, così come identificati nell’Allegato 1).

#### **1.B Potenziali aree a rischio**

In considerazione delle attività svolte dalla Società e della struttura interna adottata, ai sensi dell’art. 6 del d.lgs. 231/2001, sono individuate le seguenti categorie di operazioni ed attività a rischio, nelle quali potrebbero essere commessi i reati previsti dagli artt. 24 e 25 del d.lgs. 231/2001:

- a) predisposizione di comunicazioni riguardanti la situazione economica, patrimoniale e finanziaria della Società, ivi inclusi i bilanci e le relazioni periodiche;
- b) rilevazione, registrazione e rappresentazione dell’attività di impresa nelle scritture contabili, nei bilanci, nelle relazioni e in altri documenti di impresa;
- c) documentazione, archiviazione e conservazione delle informazioni relative all’attività di impresa;
- d) comunicazioni ad autorità pubbliche competenti;
- e) gestione dei rapporti con la società di revisione.

#### **2.B Principi di comportamento e controllo nelle principali aree di rischio**

E’ vietato porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (artt. 24 e 25 del d.lgs. 231/2001). Sono altresì proibite le violazioni dei principi e delle procedure aziendali previste nella presente Parte Speciale.

Al fine di evitare il perfezionamento dei reati societari previsti dal d.lgs. 231/2001, tutti i Destinatari devono attenersi alle seguenti condotte:

- a) agire, ciascuno secondo la propria funzione, in modo corretto, trasparente e conforme alle norme di legge, di regolamento, alle procedure aziendali esistenti, ai principi generalmente riconosciuti di tenuta della contabilità;
- b) mantenere una condotta improntata ai principi di correttezza, trasparenza e collaborazione nello svolgimento delle procedure volte alla formazione del bilancio, delle situazioni contabili periodiche e delle comunicazioni sociali in generale;
- c) mantenere una condotta improntata ai principi di correttezza, trasparenza e collaborazione nell’acquisizione, elaborazione e comunicazione delle informazioni destinate a consentire agli azionisti, alle istituzioni e al pubblico di avere un’informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della Società;

- d) assicurare il regolare funzionamento della Società e degli organi sociali, agevolando e garantendo ogni forma di controllo interno;
- e) osservare tutte le norme poste dalla legge a tutela dell'integrità del capitale sociale;
- f) rispettare, in caso di riduzione del capitale sociale, di fusione e/o di scissione, le norme di legge poste a tutela dei creditori;
- g) effettuare con tempestività, correttezza e buona fede tutte le comunicazioni previste dalla legge e dai regolamenti nei confronti delle Autorità di vigilanza, non frapponendo alcun ostacolo all'esercizio delle funzioni di controllo da queste esercitate.

In conformità a tali principi è fatto pertanto divieto di:

- a) predisporre o comunicare dati falsi o comunque suscettibili di fornire una descrizione non corretta della situazione economica, patrimoniale e finanziaria della Società;
- b) omettere di comunicare dati ed informazioni richiesti dalla normativa e dalle procedure in vigore riguardo alla situazione economica, patrimoniale e finanziaria della Società;
- c) restituire conferimenti ai soci e esentare i soci dall'effettuarli, al di fuori dei casi specificatamente previsti dalla legge;
- d) ripartire utili non effettivamente conseguiti o destinati per legge a riserva, nonché ripartire riserve che non possono essere ripartite per legge;
- e) effettuare riduzioni del capitale sociale, fusioni o scissioni in violazione delle disposizioni di legge a tutela dei creditori;
- f) procedere in ogni modo a formazione o aumento fittizi del capitale sociale;
- g) tenere comportamenti che impediscano materialmente, o che comunque ostacolino, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, lo svolgimento dell'attività di controllo o di revisione della gestione sociale da parte del collegio sindacale o della società di revisione;
- h) omettere di effettuare, con la dovuta chiarezza, completezza e tempestività, nei confronti delle autorità competenti, le comunicazioni previste per legge;
- i) porre in essere qualsiasi comportamento che sia di ostacolo all'esercizio delle funzioni da parte delle autorità pubbliche, anche in sede di ispezioni.

### **3.B *Principi per la prevenzione dei reati societari***

Per le attività nell'ambito delle categorie di operazioni a rischio sopra individuate, sono previste specifiche procedure; in particolare:

- a) ogni comunicazione esterna deve essere effettuata per iscritto e per ogni comunicazione obbligatoria per legge occorre poter ricostruire la formazione degli atti e i relativi livelli autorizzativi, a garanzia della trasparenza delle scelte effettuate;
- b) non vi deve essere identità soggettiva fra coloro che assumono o attuano le decisioni, coloro che devono dare evidenza contabile delle operazioni decise e coloro che sono tenuti a svolgere sulle stesse operazioni i controlli previsti dalla legge e dalle procedure contemplate dal sistema di controllo interno;
- c) i documenti riguardanti l'attività d'impresa devono essere archiviati e conservati, a cura della funzione competente, con modalità tali, ove richiesto dalla legge, da non permetterne la modificazione successiva, se non con apposita evidenza;
- d) nessuno tipo di pagamento può essere effettuato in contanti o in natura, salva specifica preventiva autorizzazione da parte della funzione Amministrazione Finanza e Controllo per le operazioni di cassa di importo inferiore a Euro2.500,00 (duemilacinquecento);
- e) la scelta di consulenti esterni deve essere motivata ed avvenire sulla base di requisiti di professionalità, indipendenza e competenza;
- f) i sistemi di remunerazione premianti ai dipendenti e collaboratori devono rispondere a obiettivi realistici e coerenti con le mansioni e l'attività svolta e con le responsabilità affidate;
- g) coloro che svolgono una funzione di controllo e supervisione su adempimenti connessi all'espletamento delle suddette attività devono porre particolare attenzione sull'attenzione degli adempimenti stessi e riferire immediatamente all'Organismo di Vigilanza eventuali situazioni di irregolarità.

L'Organismo di Vigilanza propone le modifiche e le eventuali integrazioni delle prescrizioni di cui sopra e delle relative procedure di attuazione.

## **PARTE SPECIALE “C”**

### ***I REATI DI OMICIDIO COLPOSO E LESIONI COLPOSE GRAVI E GRAVISSIME, COMMESSI CON VIOLAZIONE DELLE NORME ANTINFORTUNISTICHE E SULLA TUTELA DELL'IGIENE E DELLA SALUTE SUL LAVORO***

In questa *parte speciale* sono individuate le aree di attività nel cui ambito possono essere commessi i reati di omicidio colposo e lesioni colpose gravi e gravissime, di cui al d.lgs. 231/2001, così come identificati nell'Allegato 1).

#### ***1.C Potenziali aree a rischio***

In considerazione delle attività svolte dalla Società e della struttura interna adottata, ai sensi dell'art. 6 del d.lgs. 231/2001, nonché sulla base del documento di valutazione dei rischi, predisposto ai sensi del Decreto Legislativo 9 aprile 2008, n. 81 (Testo Unico Sicurezza), sono individuate le seguenti categorie di operazioni ed attività a rischio, nelle quali potrebbero essere commessi i reati previsti dagli artt. 25 *septies* del d.lgs. 231/2001:

- a) utilizzo di attrezzature non a norma;
- b) mancanza di informazione e formazione sull'attività lavorativa in particolar modo sulle attività lavorative a rischio;
- c) mancata sorveglianza dei presidi antincendio;
- d) inosservanza delle procedure di gestione delle emergenze;
- e) interventi su parti attive di impianti elettrici;
- f) accesso, transito e permanenza nei locali in uso alla Società, nello svolgimento delle sue attività da parte di dipendenti, collaboratori, agenti, fornitori, clienti e/o qualsiasi altro soggetto esterno.

#### ***2.C Principi di comportamento e controllo nelle principali aree di rischio***

E' vietato porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (artt. 25 *septies* del d.lgs. 231/2001). Sono altresì proibite le violazioni ai principi ed alle procedure aziendali previste nella presente Parte Speciale.

Al fine di evitare il verificarsi dei reati di omicidio colposo e lesioni colpose gravi e gravissime, previsti dal d.lgs. 231/2001, tutti i Destinatari devono attenersi alle specifiche regole e procedure che sono e saranno predisposte e diffuse dalla Società ai sensi del Decreto Legislativo 9 aprile 2008, n. 81 (Testo Unico Sicurezza), nonché alle seguenti condotte:

- a) osservare rigorosamente tutte le leggi e i regolamenti in materia di sicurezza sul lavoro e sulla tutela dell'igiene e salute sul lavoro che disciplinano l'accesso, il transito e lo svolgimento delle attività lavorative presso i locali in uso alla Società;

- b) partecipare ai corsi organizzati dalla Società in materia di sicurezza sul lavoro e sulla tutela dell'igiene e salute sul lavoro e sullo svolgimento delle specifiche mansioni, ai quali sono invitati;
- c) utilizzare i dispositivi di protezione individuali forniti dalla Società ai propri dipendenti, conformemente alle normative vigenti e in funzione delle mansioni svolte;
- d) segnalare alle funzioni competenti (RSPPA – responsabile dei Servizi di Prevenzione e Protezione Aziendale, RLSSA responsabile dei Lavoratori per la Sicurezza, Salute e Ambiente) ed all'Organismo di Vigilanza eventuali inefficienze dei dispositivi di protezione individuali ovvero di altri presidi a tutela della sicurezza sul lavoro e sulla tutela dell'igiene e salute sul lavoro;

In conformità a tali principi è fatto pertanto divieto di:

- a) utilizzare, nello svolgimento delle attività identificate a rischio, attrezzature, strumenti, materiali e dispositivi di protezione individuali non adeguati e non conformi alle normative vigenti per le specifiche operazioni da svolgere;
- b) disattivare o rendere anche parzialmente inefficienti dispositivi individuali o collettivi di protezione;
- c) svolgere attività ed operazioni al di fuori delle aree specificatamente identificate per gli interventi richiesti;
- d) accedere ad aree di lavoro alle quali non si è autorizzati.

### ***3.C Principi per la prevenzione dei reati di omicidio colposo e lesioni colpose gravi e gravissime***

Per le attività nell'ambito delle categorie di operazioni a rischio sopra individuate e nell'ambito specifico della gestione della sicurezza sul lavoro e della tutela dell'igiene e salute sul lavoro, nel rispetto di quanto previsto dal Decreto Legislativo 9 aprile 2008, n. 81 (Testo Unico Sicurezza), sono previste nel Documento di valutazione dei rischi specifiche procedure; in particolare:

- a) devono essere periodicamente individuati dalla Società i rischi in materia di sicurezza e tutela dell'igiene e salute sul lavoro, tenendo in adeguata considerazione: la struttura aziendale, la natura delle attività, l'ubicazione dei locali e delle aree di lavoro, l'organizzazione del personale, attrezzature e impianti;
- b) deve essere periodicamente aggiornato il documento di valutazione dei rischi adottato ai sensi del Decreto Legislativo 9 aprile 2008, n. 81 (Testo Unico Sicurezza);
- c) i lavoratori devono essere necessariamente informati circa le procedure adottate dalla Società al fine di ridurre i rischi in materia di sicurezza e tutela dell'igiene e salute sul lavoro;
- d) devono essere periodicamente definiti ed aggiornati il piano di intervento delle azioni di prevenzione e protezione sulla base del risultato della valutazione dei rischi

effettuata, nonché i programmi di informazione e formazione dei lavoratori ai fini della sicurezza e della protezione della loro salute;

- e) i dirigenti e i preposti sono tenuti a sorvegliare sull'effettivo rispetto delle procedure proposte e diffuse dalla Società e sulla adozione delle adeguate misure di prevenzione e protezione, comunicando tempestivamente eventuali eccezioni e criticità;
- f) i lavoratori in base agli specifici rischi individuati devono ricevere adeguata informazione e formazione in merito alle misure di prevenzione e protezione da adottare nello svolgimento delle proprie attività e gestione delle emergenze; per ciascun dipendente viene previsto uno specifico piano di addestramento individuale;
- g) alle ispezioni giudiziarie e amministrative devono partecipare i soggetti a ciò espressamente delegati e l'Organismo di Vigilanza dovrà essere prontamente informato sull'inizio di ogni attività ispettiva dalla direzione aziendale interessata.

## PARTE SPECIALE “D”

### *I REATI INFORMATICI*

In questa *parte speciale* sono individuate le aree di attività nel cui ambito possono essere commessi i reati informatici, di cui al d.lgs. 231/2001, così come identificati nell’Allegato 1).

#### **1.D Potenziali aree a rischio**

In considerazione delle attività svolte dalla Società e della struttura interna adottata, ai sensi dell’art. 6 del d.lgs. 231/2001, sono individuate le seguenti categorie di operazioni ed attività a rischio, nelle quali potrebbero essere commessi i reati previsti dagli artt. 24 *bis* del d.lgs. 231/2001:

- gestione e monitoraggio degli accessi ai sistemi informatici e telematici, con riferimento alle seguenti particolari attività di:
  - a) gestione del profilo utente e del processo di autenticazione;
  - b) gestione e protezione della postazione di lavoro;
  - c) gestione degli accessi verso l’esterno;
  - d) gestione e protezione delle reti;
  - e) gestione degli output di sistema e dei dispositivi di memorizzazione;
  - f) sicurezza fisica (sicurezza cablaggi, dispositivi di rete, ecc.).

#### **2.D Principi di comportamento e controllo nelle principali aree di rischio**

WELLCOMM, conscia dei continui cambiamenti delle tecnologie e dell’elevato impegno operativo, organizzativo e finanziario richiesto a tutti i livelli della struttura aziendale, si è posta come obiettivo l’adozione di efficaci politiche di sicurezza informatica; in particolare, tale sicurezza viene perseguita attraverso la protezione dei sistemi e delle informazioni dai potenziali attacchi (secondo una direttrice organizzativa, mirata alla creazione di una cultura aziendale attenta agli aspetti della sicurezza e a una direttrice tecnologica, attraverso l’utilizzo di strumenti atti prevenire e a reagire a fronte delle diverse tipologie di attacchi) e la garanzia della massima continuità del servizio.

Ciò posto, è vietato porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (artt. 24 *bis* del d.lgs. 231/2001). Sono altresì proibite le violazioni ai principi ed alle procedure aziendali previste nella presente Parte Speciale.

Al fine di evitare il verificarsi dei reati informatici, previsti dal d.lgs. 231/2001, tutti i Destinatari devono attenersi alle specifiche regole e procedure che sono e saranno predisposte e diffuse dalla Società, così come richiamate nelle dispense informative consegnate dalla Società ai dipendenti.

In particolare, è fatto divieto di:

- a) alterare documenti informatici, pubblici o privati, aventi efficacia probatoria;
- b) accedere abusivamente al sistema informatico o telematico di soggetti pubblici o privati;
- c) accedere abusivamente al proprio sistema informatico o telematico al fine di alterare e /o cancellare dati e/o informazioni;
- d) 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;
- e) 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;
- f) 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;
- g) 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;
- h) installare apparecchiature per l'intercettazione, impedimento o interruzione di comunicazioni di soggetti pubblici o privati;
- i) svolgere attività di modifica e/o cancellazione di dati, informazioni o programmi di soggetti privati o soggetti pubblici o comunque di pubblica utilità;
- j) svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui;
- k) distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità.

### **3.D *Principi per la prevenzione dei reati informatici***

Per le attività nell'ambito delle categorie di operazioni a rischio sopra individuate sono previste specifiche procedure; in particolare:

- a) utilizzare le informazioni, le applicazioni e le apparecchiature esclusivamente per motivi di ufficio;
- b) non prestare o cedere a terzi qualsiasi apparecchiatura informatica, senza la preventiva autorizzazione del Responsabile dei Sistemi Informativi;

- c) in caso di smarrimento o furto, informare tempestivamente i Sistemi Informativi e gli uffici amministrativi e presentare denuncia all'Autorità Giudiziaria preposta;
- d) evitare di introdurre e/o conservare in azienda (in forma cartacea, informatica e mediante utilizzo di strumenti aziendali), a qualsiasi titolo e per qualsiasi ragione, documentazione e/o materiale informatico di natura riservata e di proprietà di terzi, salvo acquisiti con il loro espresso consenso nonché applicazioni/software che non siano state preventivamente approvate dall'Area Sistemi Informativi o la cui provenienza sia dubbia;
- e) evitare di trasferire all'esterno dell'Azienda e/o trasmettere files, documenti, o qualsiasi altra documentazione riservata di proprietà dell'Azienda stessa o di altra società del Gruppo, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni e, comunque, previa autorizzazione del proprio Responsabile;
- f) evitare di lasciare incustodito e/o accessibile ad altri il proprio PC oppure consentire l'utilizzo dello stesso ad altre persone (famigliari, amici, etc...);
- g) evitare l'utilizzo di *passwords* di altri utenti aziendali, neanche per l'accesso ad aree protette in nome e per conto dello stesso, salvo espressa autorizzazione del Responsabile dei Sistemi Informativi; qualora l'utente venisse a conoscenza della *password* di altro utente, è tenuto a darne immediata notizia all'amministratore di sistema;
- h) evitare l'utilizzo di strumenti software e/o hardware atti a intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
- i) utilizzare la connessione a Internet per gli scopi e il tempo strettamente necessario allo svolgimento delle attività che hanno reso necessario il collegamento;
- j) rispettare le procedure e gli standard previsti, segnalando senza ritardo alle funzioni competenti eventuali utilizzi e/o funzionamenti anomali delle risorse informatiche;
- k) impiegare sulle apparecchiature dell'Azienda solo prodotti ufficialmente acquisiti dall'Azienda stessa;
- l) astenersi dall'effettuare copie non specificamente autorizzate di dati e di software;
- m) astenersi dall'utilizzare gli strumenti informatici a disposizione al di fuori delle prescritte autorizzazioni;
- n) osservare ogni altra norma specifica riguardante gli accessi ai sistemi e la protezione del patrimonio di dati e applicazioni dell'Azienda;
- o) osservare scrupolosamente quanto previsto dalle politiche di sicurezza aziendali per la protezione e il controllo dei sistemi informatici.