



BUSINESS SOLUTIONS  
TECHNOLOGY  
OUTSOURCING



***Modello di Organizzazione, di Gestione e  
Controllo  
di cui al decreto legislativo n. 231 dell'8 giugno  
2001***

***- Parte Generale -***

# ***Computer Sciences Italia srl***

## ***Modello di Organizzazione, di Gestione e Controllo***

***di cui al decreto legislativo n.  
231 dell'8 giugno 2001***

***- Parte Generale -***



**Approvato in data 2 febbraio 2006**

**Aggiornato in data 25 Giugno 2010**



## INDICE

<b>1. INTRODUZIONE</b>	<b>6</b>
1.1.DEFINIZIONI E GLOSSARIO	6
1.2.PREMESSA	9
1.3.SCOPO DEL DOCUMENTO	9
1.4.CAMPO DI APPLICAZIONE DEL DOCUMENTO	10
<b>2. IL DECRETO</b>	<b>11</b>
2.1.DESCRIZIONE	11
2.1.1. Oggetto	11
2.1.2. Caratteristiche	11
2.1.3. Il Valore Aggiunto	11
2.1.4. L'adeguatezza ed efficacia del Modello Organizzativo	12
2.2.FATTISPECIE DI REATO	12
<b>3. MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO</b>	<b>13</b>
3.1.CARATTERISTICHE DEL MODELLO	13
3.2.ARCHITETTURA DEL MODELLO ORGANIZZATIVO	13
3.3.ATTIVITÀ SENSIBILI E/O A RISCHIO REATO	14
3.4.ADOZIONE E MODIFICHE DEL MODELLO ORGANIZZATIVO	15
3.5.INTERPRETAZIONE DEL MODELLO ORGANIZZATIVO	15
3.6.MATRICE ORGANIZZATIVA E RESPONSABILITÀ	16
3.6.1. Matrice Attività/Responsabilità	16
3.6.2. Rapporti con CSC Italia	16
3.7.IL PROCESSO DI GESTIONE DEL RISCHIO	17
<b>4. PRINCIPI ED ETICA DI COMPUTER SCIENCES ITALIA SRL</b>	<b>18</b>
4.1.CODICE ETICO <i>COMPUTER SCIENCES ITALIA SRL</i>	18
4.1.1. Introduzione	18
4.1.2. Generalità	19
4.2.PRINCIPI ETICI RILEVANTI	19
4.2.1. Conformità a leggi e regolamenti	19
4.2.2. Rapporti con clienti e fornitori	20
4.2.3. Trasparenza nelle informazioni	21
4.2.4. Altri obblighi di dipendenti e Collaboratori	22
4.2.5. Pari opportunità/divieto di discriminazioni	23

4.2.6. Rapporti con la Pubblica Amministrazione	23
4.2.7. Finanziamento ai partiti politici	24
4.2.8. Sicurezza sul lavoro ed igiene ambientale	24
4.2.9. Antiriciclaggio e ricettazione	25
4.2.10. Criminalità informatica	25
4.2.11. Comunicazione all'interno di Computer Sciences Italia srl	25

## **5. L'ORGANISMO DI VIGILANZA -----27**

### **5.1.IDENTIFICAZIONE DELL'ORGANISMO DI VIGILANZA -----27**

### **5.2.REQUISITI DELL'ORGANISMO DI VIGILANZA -----27**

5.2.1. Indipendenza e autonomia	27
5.2.2. Professionalità	28
5.2.3. Autonomia nei poteri di iniziativa e controllo	28
5.2.4. Continuità di azione	28
5.2.5. Acquisizione delle informazioni	28
5.2.6. Rapporto agli Organi sociali	28

### **5.3.NOMINA DEI MEMBRI DELL'ORGANISMO DI VIGILANZA -----28**

### **5.4.RINUNCIA, REVOCA, E SANZIONI-----29**

### **5.5.FUNZIONI, ATTIVITÀ E POTERI DELL'ORGANISMO DI VIGILANZA -----30**

### **5.6.OBBLIGHI DI INFORMAZIONE VERSO L'ORGANISMO DI VIGILANZA -----31**

5.6.1. Gestione delle informazioni	32
------------------------------------	----

### **5.7.RIPORTO DELL'ORGANISMO DI VIGILANZA VERSO IL CONSIGLIO DI AMMINISTRAZIONE33**

## **6. IL SISTEMA DISCIPLINARE -----34**

### **6.1.FINALITÀ DEL SISTEMA DISCIPLINARE -----34**

### **6.2.MISURE VERSO I DIPENDENTI-----34**

### **6.3.MISURE VERSO I DIRIGENTI -----36**

### **6.4.MISURE VERSO I MEMBRI DEL CONSIGLIO DI AMMINISTRAZIONE -----36**

### **6.5.MISURE VERSO IL COLLEGIO SINDACALE -----36**

### **6.6.MISURE VERSO TERZI -----36**

## **7. FORMAZIONE, COMUNICAZIONE E DIFFUSIONE -38**

### **7.1.COMUNICAZIONE VERSO L'INTERNO-----38**

7.1.1. Comunicazione e formazione in generale	38
7.1.2. Comunicazione e formazione in materia di sicurezza e salute dei lavoratori	38
7.1.3. Comunicazione e formazione	39

### **7.2.DIFFUSIONE VERSO L'ESTERNO-----39**

# 1. INTRODUZIONE

## 1.1. DEFINIZIONI E GLOSSARIO

I seguenti termini usati nel Modello Organizzativo avranno il seguente significato	
<b>Area aziendale</b>	Si intende un settore aziendale che può comprendere una o più Funzioni aziendali.
<b>ATI</b>	Si intende l'associazione temporanea d'impresa finalizzata alla partecipazione a gare d'appalto pubbliche o alla stipulazione di contratti di appalto tra privati.
<b>Attività aziendale</b>	Si intende l'ordinaria operazione aziendale svolta nell'ambito delle mansioni attribuite alla specifica Funzione aziendale.
<b>Attività sensibile o Processo sensibile</b>	Si intende un'operazione o una serie di operazioni svolte ordinariamente dal personale dipendente nell'ambito delle proprie mansioni e che, per la loro caratteristica, richiedono l'applicazione di specifici controlli al fine di limitare l'esposizione al rischio di commissione dei reati previsti dal Decreto.
<b>Benefits &amp; Compensation</b>	Rappresenta l'attività svolta dall'Area aziendale HR finalizzata alla gestione del sistema remunerativo del personale dipendente ivi incluso il sistema premiante.
<b>Chief Information Officer (CIO)</b>	Il soggetto preposto alla gestione delle procedure informatizzate interne.
<b>Codice Etico</b>	Indica i principi etici della Società finalizzati ad evitare comportamenti che possono comportare le fattispecie di reato previste dal Decreto.
<b>Collaboratore</b>	Si intende il soggetto esterno alla Società che svolge un'attività lavorativa a tempo determinato per l'azienda in base a specifico contratto regolamentato dalla legge.
<b>Collegio Sindacale</b>	Si intende il collegio sindacale in carica della Società.
<b>Compliance SOX</b>	Si intende l'insieme delle procedure e dei controlli (prevalentemente finanziari) posti in essere per l'applicazione della normativa USA "Sarbanes – Oxley".
<b>Consigliere Delegato oppure AD</b>	Si intende il consigliere delegato in carica della Società.
<b>Consiglieri del Consiglio di Amministrazione</b>	Si intendono gli amministratori in carica della Società.
<b>Consiglio di Amministrazione oppure CdA</b>	Si intende il consiglio di amministrazione della Società.
<b>Consulente</b>	Si intende il soggetto esterno alla Società che svolge un'attività professionale non continuativa ed in piena autonomia a favore della stessa in base a specifico accordo contrattuale.
<b>Controllo interno</b>	Si intende l'insieme delle Procedure aziendali poste in essere dai Consiglieri per garantire la corretta esecuzione delle Attività aziendali, l'affidabilità, l'accuratezza e la completezza delle informazioni, nonché la salvaguardia del patrimonio aziendale.
<b>CSC Italia</b>	Si intende CSC Italia S.r.l.
<b>Data Base Administrator</b>	Si intende l'amministratore di dati – Funzione informatica che organizza e procede alla manutenzione dei dati gestiti negli archivi informatici.
<b>Decreto</b>	Indica il Decreto Legislativo 8 Giugno 2001 n° 231 e successive modificazioni e integrazioni.
<b>Direttori/Dirigenti</b>	Si intendono i lavoratori preposti alla direzione di una o più Aree aziendali con autonomia decisionale a cui compete promuovere, gestire e coordinare la realizzazione degli obiettivi aziendali.
<b>Disposizione aziendale</b>	Una regola aziendale specifica e formalizzata in termini sintetici quale, ed esempio, un ordine di servizio.
<b>Documento di valutazione dei rischi aziendali</b>	Si intende il documento di cui agli artt. 17 e 28 del D.Lgs. 81/08.
<b>Documento programmatico sulla sicurezza</b>	Si intende il documento redatto in base alle disposizioni di cui al punto 19 del disciplinare tecnico in materia di misure minime di sicurezza, allegato b del D.Lgs. n. 196 del 30 giugno 2003..
<b>F&amp;A (Finance &amp; Administration)</b>	Si intende l'Area aziendale che svolge tutte le funzioni di amministrazione e finanza per <i>Computer Sciences Italia srl</i> .
<b>Funzione aziendale</b>	Si intende una serie di attività che hanno la medesima natura, riunite tra loro perché riguardanti il medesimo oggetto operativo e finalizzate alla realizzazione degli obiettivi d'impresa.
<b>G.A. – Global Account</b>	Si intende quella categoria di clienti che fanno riferimento a contratti globali e/o definiti dal network CSC estero.

I seguenti termini usati nel Modello Organizzativo avranno il seguente significato	
<b>HR (Human Resources)</b>	Si intende l'Area aziendale che cura la gestione del personale ed il sistema assuntivo.
<b>Incaricato della Privacy</b>	Si intende la persona fisica incaricata dal titolare o dal responsabile a compiere operazioni di trattamento dei dati in base all'art. 30 del D.Lgs. n. 196 del 30 giugno 2003.
<b>Internal Application Portfolio (IAP)</b>	Funzione aziendale operante all'interno di F&A incaricata della manutenzione dei sistemi informatici applicativi.
<b>IT</b>	Si intende information technology – ovvero il settore specialistico riferito all'informatica.
<b>IWO</b>	Si tratta dell'acronimo di Intercompany Work Order: si intendono le attività lavorative italiane vs estero (e viceversa); attività lavorative Italia vs Italia; addebiti intercompany di diversa natura (es. addebiti di costi intragruppo).
<b>Legal (Legale)</b>	Si intende l'Area aziendale che cura gli aspetti giuridici connessi all'Attività aziendale.
<b>Linee Guida di Confindustria</b>	Si tratta delle linee guida per la costruzione dei modelli di organizzazione, gestione e controllo ai sensi del Decreto, approvate il 7 marzo 2002 (aggiornate al 31 marzo 2008).
<b>Mappatura dei Rischi</b>	Si intende la documentazione predisposta da <i>Computer Sciences Italia srl</i> che (i) analizza le attività "sensibili" della Società con riferimento ai rischi di commissione dei reati di cui al Decreto, (ii) ne sintetizza i protocolli posti in essere per contrastare i rischi di reato, (iii) rinvia, dove applicabile, alla documentazione più estesa dei controlli e delle procedure disponibile nel sistema aziendale, e (iv) indica analiticamente i livelli di responsabilità per la corretta applicazione delle regole aziendali.
<b>Modello Organizzativo</b>	Indica il modello di organizzazione, gestione e controllo idoneo a prevenire i reati predisposto dalla Società ai sensi del D.Lgs. 231/2001.
<b>MSS – Managed Service Sector</b>	Si intende la Funzione aziendale che (i) è incaricata della gestione complessiva dei sistemi informatici dell'azienda e dei sistemi di comunicazione (reti) con le società del gruppo (ii) fornisce prestazioni di servizi di consulenza informatica presso i clienti.
<b>Network Administrator</b>	Si intende l'amministratore di rete - Funzione informatica addetta alla gestione delle reti di comunicazione.
<b>Organigramma</b>	Si intende il sistema di rappresentazione delle varie funzioni aziendali organizzate per lo svolgimento dell'Attività aziendale secondo i relativi rapporti gerarchici intercorrenti.
<b>Organismo di vigilanza oppure OdV</b>	L'organismo dotato di autonomi poteri di iniziativa e di controllo di cui all'art. 6 del Decreto nominato dalla Società.
<b>Outsourcing</b>	Si intende l'esternalizzazione di Attività aziendali. In pratica, il ricorso ad imprese esterne per lo svolgimento di alcune Funzioni aziendali.
<b>Policy</b>	Si intende l'insieme di regole, direttive e principi stabiliti per la governance aziendale che sono anche indirizzate, direttamente o indirettamente, alla prevenzione della commissione dei reati di cui al Decreto.
<b>Procedura</b>	Un'insieme di regole aziendali codificate e da applicare nello svolgimento di una specifica Attività aziendale svolta da una Funzione aziendale incluse le Policies e i Protocolli.
<b>Processo o Ciclo</b>	Si intende l'insieme di attività interrelate o interagenti che descrivono il percorso di specifiche Attività aziendali trasformando le risorse in prodotto, sia esso un bene, un servizio o un'informazione o una combinazione di tali elementi. Il processo aziendale può coinvolgere diverse Aree aziendali o Funzioni aziendali.
<b>Procurement</b>	Si intende la Funzione aziendale che è preposta allo svolgimento dell'attività di acquisizione di beni e di servizi.
<b>Protocolli o Controlli preventivi</b>	Si intendono le regole di controllo previste nello svolgimento di un'Attività aziendale e finalizzati a contrastare i rischi di commissione dei reati di cui al Decreto.
<b>Pubblica Amministrazione oppure P.A.</b>	Si intende quanto previsto al paragrafo 3.1.1 della Parte "A" – <i>Reati contro la Pubblica Amministrazione</i> all'interno della Parte Speciale del presente Modello Organizzativo.
<b>Recruiting</b>	Si intende l'attività svolta nell'ambito dell'Area aziendale HR che cura il sistema assuntivo del personale dipendente.
<b>Regolamento</b>	Regolamento di funzionamento dell'Organismo di vigilanza predisposto dal medesimo.
<b>Responsabile dell'Area aziendale</b>	Si intendono i soggetti a cui è affidata la responsabilità di una specifica Area aziendale come descritte nell'Organigramma.
<b>Responsabile della Funzione aziendale</b>	Si intende il soggetto a cui è affidata la responsabilità di una specifica Funzione aziendale inseriti all'interno delle Aree aziendali che compongono l'Organigramma.
<b>Responsabile della Privacy</b>	Si intende la persona preposta dal titolare del trattamento dei dati personali in base all'art. 29 del del D.Lgs. n. 196 del 30 giugno 2003.
<b>Risk Management Process</b>	Si tratta del processo di valutazione dei rischi aziendali.
<b>RSPP</b>	Si tratta del responsabile del servizio di prevenzione e protezione di cui all'art. 2 lett. f) del TU.
<b>RTI</b>	Si intende il raggruppamento temporaneo d'impresе finalizzato alla partecipazione a gare d'appalto pubbliche o alla stipulazione di contratti di appalto tra privati.

I seguenti termini usati nel Modello Organizzativo avranno il seguente significato	
<b>S&amp;MD (Funzione Marketing)</b>	Si intende l'Area aziendale che promuove e coordina le iniziative di immagine e promozione della Società.
<b>SGPA</b>	Si intende il Sistema di Governo dei Processi e Policies Aziendali posto in essere dalla Società..
<b>Sindaci</b>	Si intendono i sindaci in carica della Società.
<b>Sistema di governance</b>	Si intende l'insieme di regole di ogni livello che disciplinano per legge o per disposizioni aziendali la gestione dell'impresa.
<b>Sistema disciplinare</b>	Si intende il sistema disciplinare di cui agli artt. 6 e 7 del Decreto idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello Organizzativo.
<b>Società o Computer Sciences Italia srl</b>	Indica <i>Computer Sciences Italia srl</i>
<b>Società del gruppo CSC</b>	Si intende società controllanti la Società o correlate alla Società.
<b>Soggetti Apicali</b>	Si intendono le persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso di cui al l'art. 5, comma 1, lett. a) del Decreto.
<b>Soggetti Subordinati</b>	Si intendono le persone sottoposte alla direzione o alla vigilanza di uno dei Soggetti Apicali di cui al l'art. 5, comma 1, lett. b) del Decreto.
<b>Soggetti destinatari</b>	Sono i soggetti sia dipendenti che terzi rispetto alla Società ai quali sono indirizzati i principi etici, le istruzioni operative ed il Modello Organizzativo nel suo insieme, ciascuno secondo i livelli di responsabilità a loro attribuiti.
<b>Success fees</b>	Si intende la remunerazione che si matura, laddove contrattualmente pattuita, al raggiungimento di un obiettivo aziendale.
<b>System Administrator</b>	Si intende l'amministratore di sistema. Si tratta della funzione informatica che organizza, aggiorna e procede alla manutenzione dei sistemi operativi.
<b>Testo Unico in materia di salute e sicurezza sul lavoro oppure TU</b>	Si intende il D.Lgs. n. 81/2008 "Attuazione dell'articolo 1 della legge 3 agosto 2007, n. 123, in materia di tutela della salute e della sicurezza nei luoghi di lavoro".
<b>Ufficio</b>	E' un settore specifico di una Funzione aziendale incaricata di svolgere una o più attività inerenti alla Funzione stessa.

## 1.2. PREMESSA

**1.2.1** – Il decreto legislativo 8 Giugno 2001 n°231 ha introdotto nel nostro ordinamento la disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica. In base a tale nuova disciplina, nel caso in cui vengano commessi i reati previsti nel Decreto e secondo le condizioni ivi specificate, la Società (in quanto entità legale) può essere ritenuta direttamente responsabile, a meno che non dimostri di avere adottato un modello di organizzazione, di gestione e di controllo tale per cui l'azione sia stata commessa da una singola persona, in violazione alle disposizioni aziendali.

*Computer Sciences Italia srl* ha adottato il presente Modello Organizzativo, con delibera del Consiglio di Amministrazione del 2 Febbraio 2006.

**1.2.2** – *Computer Sciences Italia srl* confida sull'integrità del comportamento di tutti i propri dipendenti per mantenere un idoneo livello di applicazione delle disposizioni previste dal presente Modello Organizzativo. Conseguentemente, il mancato rispetto (in tutto o in parte) delle disposizioni definite nel presente Modello Organizzativo (e delle altre disposizioni correlate), sarà considerato da *Computer Sciences Italia srl* come un abuso della fiducia riposta nei confronti del dipendente che non rispetta le direttive aziendali. Pertanto, la non osservanza di dette disposizioni potrà comportare l'applicazione di appropriate sanzioni disciplinari.

## 1.3. SCOPO DEL DOCUMENTO

**1.3.1** - Il presente documento costituisce e descrive il Modello Organizzativo per la prevenzione dei reati previsti nel Decreto.

**1.3.2** - Il presente Modello Organizzativo, è elaborato tenendo in considerazione l'interazione del sistema SGPA e del complesso delle Policies e dei regolamenti formalizzati in *Computer Sciences Italia srl* con la disciplina e le previsioni del Decreto.

L'obiettivo è quello di integrare il complesso delle norme di condotta, principi, Policies e Procedure di CSC, nonché, tutti gli strumenti organizzativi e i Controlli preventivi esistenti per dare attuazione alle prescrizioni del Decreto.

Questo permette:

- il mantenimento del Sistema di governance già in essere; agendo sui Processi che, direttamente o indirettamente, possono influenzare il sistema di gestione aziendale proprio di *Computer Sciences Italia srl* e il Modello Organizzativo;
- di adottare, successivamente, anche altri Sistemi di governance (normativi, cogenti o volontari) sempre in maniera integrata.

Il presente documento, costituisce il primo punto di riferimento per valutare l'idoneità di *Computer Sciences Italia srl* alle prescrizioni dettate dal Decreto.

## 1.4. CAMPO DI APPLICAZIONE DEL DOCUMENTO

**1.4.1** - Il presente Modello Organizzativo è applicabile per tutte le sedi di *Computer Sciences Italia srl*, sede legale Centro Direzionale Milanofiori, Strada 3 Palazzo b1, Assago-Milano (Reg. Imp. Mi e C.F.12151170151).

**1.4.2** – Le prescrizioni del presente documento si applicano a tutti i dipendenti di *Computer Sciences Italia srl* che, a qualsiasi titolo, sono partecipi e/o gestiscono i Processi ed attività di riferimento, e/o dati e informazioni connesse e, ove applicabili, nei confronti di tutti i Soggetti destinatari.

Infatti, secondo il Decreto, la Società è responsabile per i reati commessi nel suo interesse o a suo vantaggio:

- da Soggetti Apicali;
- da Soggetti Subordinati.

*Computer Sciences Italia srl* non risponde, per espressa previsione legislativa (art. 5, comma 2, Decreto), se le persone indicate hanno agito nell'interesse esclusivo proprio o di terzi.

**1.4.3** – Il presente documento sarà soggetto a revisione periodica da parte di *Computer Sciences Italia srl*, per opera dell'Organismo di vigilanza e/o del Consiglio di Amministrazione, in funzione del principio del miglioramento continuo posto alla base del sistema di governo dei processi aziendali.

Il Modello Organizzativo quindi, potrà subire delle modifiche a discrezione della Società stessa a seguito di modifiche derivanti dall'osservanza delle norme giuridiche in materia e loro integrazioni e variazioni.

In ogni caso, i principi e le metodologie del presente Modello Organizzativo definito da *Computer Sciences Italia srl* troveranno applicazione anche con riferimento a eventuali ulteriori ipotesi di reato che, a seguito di intervento legislativo dovessero assumere rilievo in ordine alla responsabilità amministrativa della Società.

## 2. IL DECRETO

### 2.1. DESCRIZIONE

#### 2.1.1. Oggetto

Con il Decreto si introduce nel nostro ordinamento giuridico il principio della responsabilità amministrativa delle persone giuridiche, quando specifici reati sono commessi dai Soggetti Apicali o dai Soggetti Subordinati, qualora tali reati siano stati commessi nell'interesse o a vantaggio della Società stessa (superamento del principio "*societas delinquere non potest*").

Tale responsabilità si aggiunge a quella della persona fisica che ha realizzato materialmente il reato.

#### 2.1.2. Caratteristiche

Le società si spingono sempre più verso la definizione di piani e programmi tendenti alla prevenzione di eventi dannosi per le stesse; per cui la previsione di un Modello Organizzativo permette di dare le indicazioni necessarie a prevenire l'insorgere di potenziali criticità, definendo ove possibile, opportuni indicatori per le singole tipologie di rischio.

A tal fine Confindustria ha emanato le Linee Guida di Confindustria per la costruzione di modelli organizzativi ai sensi del Decreto.

In estrema sintesi, possiamo riassumere le aree di intervento individuate nelle Linee Guida di Confindustria, come segue:

- individuazione degli ambiti aziendali di attività e dei vari processi a rischio (operazioni contabili, attività di business, etc.);
- individuazione dei rischi potenziali e delle condizioni per la commissione di reati nell'interesse o a vantaggio della società;
- nomina di un organismo di vigilanza che sia a diretto riporto del vertice interno aziendale, indipendente, autorevole, adeguato, autonomo, non occasionale;
- definizione di responsabilità e attività finalizzate alla appropriata gestione delle attività;
- definizione di processi e procedure interne, atte a governare, prevenire e controllare le attività a rischio;
- definizione dei meccanismi di comunicazione da parte dell'organismo di vigilanza verso i vertici della società e viceversa;
- definizione dei meccanismi di comunicazione da parte dei soggetti destinatari del Decreto verso l'organismo di vigilanza e viceversa;
- predisposizione di un codice etico;
- previsione di un sistema disciplinare e dei meccanismi sanzionatori, in caso di violazione del modello organizzativo.

#### 2.1.3. Il Valore Aggiunto

Dotare la Società un Modello Organizzativo atto a prevenire i reati, costituisce una scelta strategica per la Società stessa e per i soci, dando la possibilità di:

- poter perfezionare l'organizzazione interna ottimizzando la suddivisione di competenze e responsabilità;
- poter assicurare il rispetto degli adempimenti previsti dal Decreto ogni qualvolta ciò venga richiesto nell'ambito dei rapporti contrattuali (es. gare pubbliche);
- migliorare l'immagine presso i clienti, il mercato e verso l'esterno in generale.

Oltre al valore aggiunto derivante dall'implementazione di un Sistema di governance il Decreto prevede la possibilità di andare esenti dalle responsabilità e dalle conseguenti sanzioni quando si verifica un procedimento penale per uno dei reati previsti dal Decreto, nel caso il Modello Organizzativo venga efficacemente adottato.

### **2.1.4. L'adeguatezza ed efficacia del Modello Organizzativo**

È importante evidenziare che l'accertamento della responsabilità della Società viene effettuato anche attraverso la valutazione della adeguatezza ed efficacia del Modello Organizzativo e, quindi, il giudizio d'idoneità del sistema interno di organizzazione, gestione e controllo per la prevenzione dei reati che il giudice è chiamato a formulare in occasione di un procedimento penale.

## **2.2. FATTISPECIE DI REATO**

Le fattispecie di reato previste dal Decreto, che possono configurare la responsabilità amministrativa della Società, sono quelle espressamente previste e sono comprese nelle seguenti categorie:

- reati contro la Pubblica Amministrazione (quali corruzione e malversazione ai danni dello Stato, indebita percezione di erogazioni, truffa ai danni dello Stato e frode informatica ai danni dello Stato, indicati agli artt. 24 e 25 del Decreto);
- reati societari (quali, ad esempio, false comunicazioni sociali, falso in prospetto, illecita influenza sull'assemblea, indicati all'art. 25 ter del Decreto);
- reati transnazionali (quali, ad esempio, associazione a delinquere o associazione di tipo mafioso con estensione e ramificazione in più nazioni, previsti dall'art. 10 della Legge 146/2006);
- reati di falso nummario (quali, ad esempio, falsificazione di monete, indicati dall'art. 25 bis del Decreto);
- reati in materia di antiriciclaggio (quali, ad esempio, riciclaggio di denaro o ricettazione indicati dall'art. 25 octies del Decreto);
- reati in materia di salute e sicurezza sul lavoro (indicati dall'art 25 septies del Decreto, materia disciplinata anche dall'art. 30 del D.Lgs n. 81/2008);
- reati in materia di criminalità informatica (quali, ad esempi, accessi non autorizzati, violazioni di sistemi informatici o falsificazioni di documenti informatici, indicati all'art. 24 bis del Decreto);
- delitti in materia di terrorismo e di eversione dell'ordine democratico (ivi incluso l'assistenza agli associati, indicati all'art. 25 quater del Decreto);
- delitti contro la personalità individuale (quali, ad esempio, l'induzione alla prostituzione, la pornografia minorile, la tratta di persone e la riduzione e mantenimento in schiavitù, indicati all'art. 25 quinquies del Decreto);
- abusi di mercato: abuso di informazioni privilegiate e manipolazione del mercato (art. 25 sexies del Decreto);
- pratiche di mutilazione degli organi genitali femminili (art. 25 quater.1 del Decreto).

La Società può essere chiamata a rispondere in Italia in relazione ai reati contemplati nel Decreto, anche se commessi all'estero, nei casi e alle condizioni previsti dagli articoli 7, 8, 9 e 10 del codice penale e purché nei suoi confronti non proceda lo Stato del luogo in cui e' stato commesso il fatto.

## 3. MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

### 3.1. CARATTERISTICHE DEL MODELLO

Il Decreto (art. 6), prevede che il Modello Organizzativo abbia determinate caratteristiche, tali da far sì che possa essere addotto a esimente della responsabilità dell'ente in caso di commissione dei reati; inoltre, tali caratteristiche, di seguito elencate, guidano l'implementazione stessa del Modello Organizzativo:

- Mappatura dei Rischi: consiste nell'analisi del contesto aziendale, di Processi e prassi, per evidenziare in quale Area aziendale ovvero Attività aziendale e secondo quali modalità si possono verificare eventi pregiudizievoli per gli obiettivi indicati dal Decreto;
- progettazione del sistema di controllo (c.d. Protocolli): si sostanzia nella valutazione del Sistema di governance esistente all'interno della Società in termini di capacità di contrastare/ridurre efficacemente i rischi identificati, operando l'eventuale adeguamento del sistema stesso;
- individuazione delle modalità di gestione delle risorse finanziarie idonee a impedire la commissione dei reati;
- previsione degli obblighi di informazione dell'Organismo di vigilanza: si sostanzia nell'istituzione dell'organo di Controllo interno posto a monitorare e verificare il funzionamento e l'osservanza del Modello Organizzativo, avente anche il compito di curare l'eventuale aggiornamento. Il Modello Organizzativo deve prevedere anche un sistema informativo costante dell'Organismo di vigilanza;
- previsione di un'attività di monitoraggio sistematico: diretta a far sì che periodicamente il funzionamento del Modello Organizzativo venga opportunamente verificato;
- previsione un'attività di comunicazione e diffusione del Modello Organizzativo;
- definizione di un appropriato Sistema disciplinare e sanzionatorio: da applicare nel caso di mancato rispetto delle disposizioni previste dal Modello Organizzativo, nei confronti dell'eventuale autore del reato che abbia agito eludendo fraudolentemente le disposizioni del Modello Organizzativo.

### 3.2. ARCHITETTURA DEL MODELLO ORGANIZZATIVO

Il Modello Organizzativo definito da *Computer Sciences Italia srl*, si compone di:

- Una **Parte Generale**, che definisce i principi, le logiche e la struttura del Modello Organizzativo;
- Una **Parte Speciale**, nella quale sono illustrate le categorie dei reati contemplati dal Decreto evidenziando le tipologie potenzialmente applicabili, quelle associabili ad un livello di rischio molto basso o remoto e quelle ritenute non applicabili tenuto conto della realtà operativa di *Computer Sciences Italia srl*.

È parte del presente Modello Organizzativo anche la Mappatura dei Rischi con evidenza, per ciascun reato considerato delle seguenti componenti:

- l'Area aziendale o la Funzione aziendale potenzialmente coinvolta;
- il Processo o l'Attività sensibile a rischio reato;
- la descrizione sintetica dei Protocolli/Controlli preventivi da seguire e/o regole specifiche da osservare;
- i responsabili di primo e secondo livello dell'applicazione costante delle misure di controllo;
- il riferimento alla specifica Policy, Protocollo o Procedura aziendale;
- la valutazione del grado di rischio (H = alto, M = medio L = basso).

### 3.3. ATTIVITÀ SENSIBILI E/O A RISCHIO REATO

A seguito dell'analisi effettuata nel contesto organizzativo ed operativo di *Computer Sciences Italia srl*, finalizzata alla individuazione delle aree che potenzialmente possono rivelare il rischio di commissione dei reati previsti dal Decreto, si può affermare che le attività a rischio reato in *Computer Sciences Italia srl* possono essere circoscritte a:

- i reati contro la Pubblica Amministrazione (salvo le fattispecie evidenziate nella Parte A) della Parte Speciale);
- i reati societari (salvo alcune fattispecie evidenziate nella Parte B della Parte Speciale);
- i reati in materia di antiriciclaggio;
- i reati in materia di salute e sicurezza sul lavoro;
- i reati in materia di criminalità informatica (salvo alcune fattispecie evidenziate nella Parte E della Parte Speciale).

All'interno della realtà aziendale di *Computer Sciences Italia srl* le Attività sensibili sono definite e formalizzate nell'apposito documento di Mappatura dei Rischi.

Si riassumono di seguito le principali aree sensibili su cui viene posta la necessaria attenzione in relazione alla prevenzione dei reati indicati nel Decreto mentre si rimanda sempre al citato documento di Mappatura dei Rischi per una analisi e definizione puntuale di tutte le Attività aziendali, Processi, Aree aziendali e/o Funzioni aziendali a rischio per i reati previsti dal Decreto.

Riguardo ai Processi/Attività aziendali a rischio per i reati contro la Pubblica Amministrazione sono considerate a titolo esemplificativo, ma non esaustivo:

- le attività che comportano rapporti con la Pubblica Amministrazione nella normale gestione d'impresa (ASL, Uffici del lavoro, Uffici fiscali, ecc.);
- il ricorso a finanziamenti pubblici (esempio: gestione finanziamenti, contributi e/o benefici pubblici);
- una serie di attività amministrative (esempio: contabilità fornitori, uscite finanziarie, gestione di commessa, fatturazione attiva);
- le attività rientranti nella sfera dell'amministrazione del personale (esempio: recruiting, benefits & compensation);
- le attività di acquisizione di beni e servizi (ivi incluse la qualificazione dei fornitori e l'utilizzo di Consulenti/subcontractors).

Riguardo ai Processi/Attività aziendali a rischio per i reati societari sono considerate a titolo esemplificativo, ma non esaustivo;

- le attività seguite per la redazione del bilancio civilistico e consolidato;
- la fatturazione (ciclo attivo);
- la fatturazione (ciclo passivo);
- la gestione di tesoreria;
- le procedure di contabilità generale.

Riguardo ai Processi/Attività a rischio per i reati in materia di antiriciclaggio sono considerate:

- le attività connesse agli acquisti di beni e servizi;
- le attività connesse alle uscite finanziarie;
- le attività relative agli incassi.

Riguardo ai Processi/Attività aziendali a rischio per i reati in materia di salute e sicurezza sul lavoro sono considerate:

- le attività di monitoraggio in tema di nomina delle figure professionali previste dal TU;
- la formalizzazione e l'aggiornamento periodico del documento di valutazione dei rischi aziendali di cui agli artt. 17 e 28 del TU;
- le attività formative obbligatorie.

Riguardo ai Processi/Attività aziendali a rischio per i reati in materia di criminalità informatica sono considerate a titolo esemplificativo, ma non esaustivo:

- le attività che regolano l'accesso ai sistemi, PC e risorse contenenti dati aziendali;
- l'utilizzo dei mezzi di comunicazione elettronica (internet, posta elettronica, etc.);
- le attività che regolano l'accesso alle reti ed ai sistemi esterni.

### **3.4. ADOZIONE E MODIFICHE DEL MODELLO ORGANIZZATIVO**

Il Modello Organizzativo di *Computer Sciences Italia srl* è adottato dal Consiglio di Amministrazione e tutte le modifiche sostanziali del Modello Organizzativo derivanti, ad esempio, dall'introduzione di nuovi reati o quelle attinenti alla valutazione del rischio, sono di competenza del Consiglio di Amministrazione.

A tale scopo l'OdV porterà all'attenzione del Consiglio di Amministrazione le modifiche al Modello Organizzativo che si rivelassero necessarie e potrà avvalersi, per l'espletamento di tale compito, della struttura interna della Società.

Le modifiche alla Mappatura dei Rischi, ad eccezione del livello dei rischi, sono concordate fra l'OdV e il Responsabile dell'Area aziendale interessata.

### **3.5. INTERPRETAZIONE DEL MODELLO ORGANIZZATIVO**

L'interpretazione del presente Modello Organizzativo è affidata a:

- Organismo di vigilanza;
- Consiglio di Amministrazione.

## 3.6. MATRICE ORGANIZZATIVA E RESPONSABILITÀ

### 3.6.1. Matrice Attività/Responsabilità

Di seguito, in maniera schematica, una tabella riassuntiva con alcune delle principali attività poste in essere dalla Società al fine di adempiere alle disposizioni del Decreto correlate ai soggetti o organi responsabili:

TASKS PRINCIPALI	SOGGETTI O ORGANI RESPONSABILI					
	CdA	OdV	Responsabili di Area aziendale	Dirigenti	Dipendenti	Terze parti
Adozione Modello Organizzativo	<input checked="" type="checkbox"/>					
Accettazione e sottoscrizione del Modello Organizzativo			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Nomina Organismo di vigilanza e suoi membri	<input checked="" type="checkbox"/>					
Accettazione e messa in atto delle regole e adempimenti previsti nel rispetto delle Policies e Procedure di CSC.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Comunicazione e diffusione Modello Organizzativo	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
Valutazione della modifica/adeguamento Modello Organizzativo	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				
Realizzazione nuove Policies/Procedure finalizzate ai contenuti del Decreto		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
Approvazione delle modifiche al Modello Organizzativo	<input checked="" type="checkbox"/>					
Segnalazione di qualsiasi atto/attività che induca (anche potenzialmente) un possibile rischio reato	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Aggiornamento e formazione continua sul Modello Organizzativo		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Table 1 – Matrice schematica attività/responsabilità

### 3.6.2. Rapporti con CSC Italia

CSC Italia S.r.l. e *Computer Sciences Italia srl* hanno stipulato un Accordo di Servizi in base al quale:

- *Computer Sciences Italia srl* si impegna a fornire determinati servizi elencati all'art. 1 dell'Accordo di Servizi in favore di CSC Italia tra i quali, a titolo esemplificativo, il servizio di consulenza ed assistenza (i) in relazione all'attività di contabilizzazione, tenuta dei libri e dei registri contabili, (ii) nelle relazioni esterne di CSC Italia connesse alle attività commerciali gestite da *Computer Sciences Italia srl*;
- CSC Italia si impegna a fornire alcuni servizi in favore di *Computer Sciences Italia srl*.

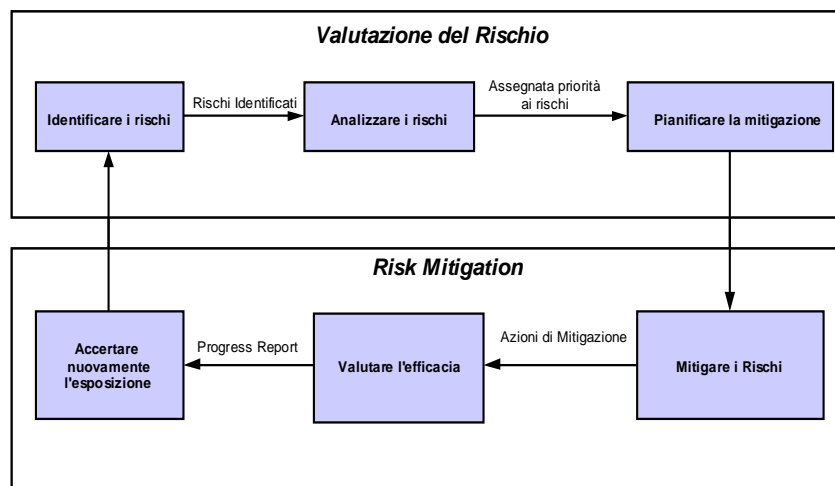
Di conseguenza, nell'ottica del rispetto del Decreto, CSC Italia e *Computer Sciences Italia srl* si sono impegnate, nell'esecuzione delle attività oggetto dell'Accordo di Servizi, al rispetto delle norme di comportamento, delle procedure e dei controlli previsti dai rispettivi Modelli Organizzativi ai sensi del Decreto e faranno in modo che ciascuno dei propri dipendenti svolga le proprie mansioni nel rispetto di tale principio. In caso di inadempimento le parti avranno facoltà di richiedere la sospensione dei servizi, salvo il diritto a chiedere il risarcimento del danno subito.

### 3.7. IL PROCESSO DI GESTIONE DEL RISCHIO

Il Risk Management Process, che si applica alla valutazione dei rischi rilevante ai fini del Decreto, in *Computer Sciences Italia srl* è un processo iterativo, come illustrato nella tabella seguente.

Questo processo si applica all'inizio di ciascuna attività e si ripete per tutto il ciclo di vita dell'attività di riferimento. La gestione dei rischi è composta di sei attività raggruppate in due aree principali:

- **Valutazione**
  - Identificazione dei rischi
  - Analisi dei rischi
  - Pianificazione della mitigazione dei rischi
- **Mitigazione**
  - Attuazione delle strategie di mitigazione
  - Valutazione dell'efficacia delle azioni attuate
  - Rivalutazione dell'esposizione al rischio



La metodologia sopra indicata corrisponde al percorso logico che risulta riportato nella Parte Speciale del Modello Organizzativo laddove si esaminano i reati previsti dal Decreto, il grado di loro applicabilità alla realtà aziendale e, conseguentemente, nella Mappatura dei Rischi.

## **4. PRINCIPI ED ETICA DI COMPUTER SCIENCES ITALIA SRL**

### **4.1. CODICE ETICO COMPUTER SCIENCES ITALIA SRL**

#### **4.1.1. Introduzione**

Il presente codice contiene le regole di etica e di condotta aziendale che i Soggetti destinatari sono tenuti ad osservare nello svolgimento delle Attività aziendali.

Il Codice Etico evidenzia, altresì, i comportamenti ritenuti non etici che la Società intende scoraggiare in quanto considerati difformi dai principi contenuti nel Codice Etico.

La Società provvede a comunicare ed informare tutti i Soggetti destinatari dell'adozione del presente Codice Etico, e del suo contenuto, che sarà divulgato anche a mezzo di un estratto, raccomandandone la puntuale osservanza.

In particolare, la Società provvede, attraverso l'istituzione dell'Organismo di vigilanza (di cui al successivo capitolo 5) a:

- informare tutti i Soggetti destinatari dell'adozione del Codice Etico;
- interpretare e chiarire le disposizioni e le Procedure aziendali contenute nel Codice Etico;
- verificare l'effettiva osservanza del Codice Etico da parte di tutti i Soggetti destinatari;
- aggiornare e modificare il Codice Etico, nonché adeguarlo alle esigenze della Società.

La Società, al fine di assicurare un effettivo rispetto delle regole previste dal Codice Etico, ha predisposto un efficace Sistema disciplinare in caso di violazione delle stesse.

Resta ferma la responsabilità del Consiglio di Amministrazione di controllare l'adesione al Codice Etico e di assicurarne l'applicazione attraverso i Protocolli e le Policies predisposti dalla Società.

Ai Responsabili di ciascuna Area aziendale (HR, F&A, Legal, S&MD), nell'ambito della rispettive strutture organizzative, è demandato il compito della corretta divulgazione ed effettiva applicazione dei principi contenuti nel presente Codice Etico.

Al fine di permettere la verifica dell'osservanza del Codice Etico, l'aggiornamento dello stesso e l'irrogazione delle sanzioni ai soggetti che lo violano, qualsiasi trasgressione commessa da un Soggetto destinatario va segnalata tempestivamente al Responsabile dell'Area aziendale di appartenenza e all'OdV.

La Società ha adottato il presente Codice Etico non solo allo scopo di dare attuazione a quanto previsto dalle disposizioni del Decreto ma soprattutto a presidio della propria reputazione e immagine sul mercato di riferimento, ed al fine di diffondere i valori d'impresa ed i principi fondamentali di correttezza professionale, integrità personale, tutela della salute nell'ambiente di lavoro, nonché di trasparente competizione sul mercato da parte di tutti i soggetti che vi operano.

In tale prospettiva, il presente Codice Etico, nel tener conto dei suggerimenti formulati nelle Linee Guida di Confindustria, rappresenta una conferma delle regole e dei principi-guida cui la Società intende fare costante riferimento nell'esercizio delle proprie attività imprenditoriali.

Per tutti i motivi sopra specificati, si segnala che l'osservanza del Codice Etico è da considerarsi parte integrante delle obbligazioni contrattuali assunte dai dipendenti ai sensi e per gli effetti di cui all'art. 2104 del codice civile.

La violazione delle norme del Codice Etico potrà pertanto costituire inadempimento grave alle obbligazioni derivanti dal contratto di lavoro e fonte di illecito civile, con ogni conseguente responsabilità personale.

Analogamente, la Società si riserva di tutelare i propri interessi in ogni sede competente avverso i terzi (fornitori, agenti e consulenti ecc.) che abbiano violato le norme del presente Codice Etico a loro destinate e che abbiano formato oggetto di pattuizione contrattuale con la Società.

Le risorse umane della Società, ad ogni livello gerarchico o di responsabilità funzionale, nonché i terzi (ove a ciò tenuti contrattualmente), sono quindi chiamati ad una scrupolosa osservanza delle norme e delle regole di condotta contenute nel presente Codice Etico e delle prescrizioni previste nelle Linee Guida di Confindustria.

È importante sottolineare che il gruppo multinazionale a cui *Computer Sciences Italia srl* appartiene ha altresì adottato i Code of Ethics di seguito elencati, resi disponibili attraverso i repository aziendali, via web e/o attraverso la intranet aziendale:

- CSC - Code of Ethics and standard of conducts
- CSC - Code for Ethics for the CEO, CFO and CAO
- CSC - Code of Ethics for Directors and Employees

Tali documenti rappresentano uno strumento adottato in via autonoma al fine di esprimere i principi di deontologia aziendale riconosciuti come propri del Gruppo e suscettibile di applicazione sul piano generale da parte di tutte le società del Gruppo e di tutto il personale *Computer Sciences Italia srl*.

Nell'ambito degli stessi sono rinvenibili anche alcuni dei principi del presente Codice Etico di *Computer Sciences Italia srl*, unitamente agli altri principi applicabili e rilevanti ai fini del Decreto. Si precisa che in ogni caso, ai fini dell'applicazione ed interpretazione del Decreto, prevalgono le regole ed i principi di cui al presente Codice Etico.

## **4.1.2. Generalità**

Ciò che contraddistingue la Società è il perseguimento dell'eccellenza a livello tecnico e dei più elevati standard di professionalità.

Il Codice Etico di *Computer Sciences Italia srl* conferma l'impegno della Società verso un comportamento etico nella conduzione delle proprie attività commerciali.

Siamo orgogliosi della nostra dedizione all'integrità, alla correttezza e alla responsabilità sociale.

In *Computer Sciences Italia srl* nessuno potrà mai giustificare un'azione non etica, o illegale, basandola sul fatto di aver seguito ordini ricevuti.

Tutti sono ritenuti responsabili delle proprie azioni come individui e come rappresentanti della Società.

I principi presentati nel Codice Etico riflettono il tipo di comportamento che ci ha permesso di ottenere il rispetto e il successo di cui godiamo oggi.

Mentre ci apprestiamo a stabilire obiettivi ancora più alti per *Computer Sciences Italia srl*, è fondamentale ricordare che la nostra Società si basa su una stretta aderenza a una condotta etica in tutti i nostri rapporti di lavoro.

Fare diversamente non è accettabile!

Il Consiglio di Amministrazione della Società è responsabile del controllo relativo all'applicazione dei principi di etica e condotta aziendale attraverso il sistema dei Protocolli e Policies a tal fine predisposti dalla Società. I Dirigenti ad ogni livello sono responsabili della comunicazione e dell'applicazione effettiva di questi principi nell'ambito delle rispettive strutture organizzative.

Qualora sorgessero dubbi circa l'interpretazione e/o l'applicazione del Codice Etico, si suggerisce di consultare il responsabile dell'Area aziendale HR al fine di ottenere chiarimenti in merito.

Qualora entro un ragionevole termine, il responsabile dell'Area aziendale HR non fornisca al richiedente risposte esaurienti, le medesime richieste potranno essere rivolte all'Organismo di vigilanza, di cui al successivo capitolo 5.

## **4.2. PRINCIPI ETICI RILEVANTI**

### **4.2.1. Conformità a leggi e regolamenti**

#### **4.2.1.1. Rispetto delle Leggi**

*Computer Sciences Italia srl* riconosce come principio imprescindibile il rispetto delle leggi e regolamenti vigenti (sia nazionali che esteri), con particolare riferimento alle leggi a tutela della salute, dell'integrità morale e della dignità dei dipendenti e collaboratori, della privacy, della sicurezza nei luoghi di lavoro e dell'ambiente.

A tal fine, ogni dipendente di *Computer Sciences Italia srl* si impegna al rispetto delle leggi e dei regolamenti vigenti in tutti i paesi in cui opera.

Tale impegno è valevole per tutti i Soggetti destinatari ai quali si chiede di prendere attenta visione del contenuto del Codice Etico.

*Computer Sciences Italia srl* inoltre, in quanto appartenente ad un gruppo multinazionale con casa madre americana è particolarmente attenta alla compliance e conformità ai principi espressi dal U.S. *Foreign Corrupt Practices Act (FCPA)*, sia da parte del proprio personale che da parte dei terzi con cui compie attività di business.

#### **4.2.1.2. Integrità e tutela della persona**

La Società si impegna a tutelare l'integrità morale dei dipendenti e Collaboratori garantendo il diritto a condizioni di lavoro rispettose della dignità della persona. Pertanto, la Società salvaguarda i propri dipendenti e/o Collaboratori da atti di violenza psicologica, e contrasta qualsiasi atteggiamento o comportamento discriminatorio o lesivo della persona, delle sue opinioni e delle sue preferenze.

Non sono consentite o tollerate molestie sessuali e devono essere evitati comportamenti o discorsi che possano turbare la sensibilità della persona (i.e., l'esposizione di immagini con espliciti riferimenti sessuali, allusioni insistenti e continuate).

I dipendenti e/o Collaboratori, che ritengano di essere stati oggetto di molestie o di essere stati discriminati per qualsivoglia motivo, sono legittimati a segnalare l'accaduto al responsabile gerarchico o all'Organismo di vigilanza, che – condotte le opportune indagini - valuteranno l'effettiva violazione del Codice Etico e adotteranno i provvedimenti ritenuti più opportuni.

### **4.2.2. Rapporti con clienti e fornitori**

#### **4.2.2.1. Relazioni con i clienti e fornitori**

I dipendenti ed i Collaboratori della Società che hanno contatti con i clienti e con i fornitori devono cercare di comprendere le loro richieste e fare ciò che è ragionevolmente fattibile per soddisfarle. La Società ritiene che onestà ed affidabilità morale siano doti essenziali per stabilire buoni e duraturi rapporti con i clienti e fornitori. Le dichiarazioni rese e le informazioni fornite ai clienti ed ai fornitori in ordine a soluzioni, servizi, consulenze o prezzi, dovranno essere rispondenti al vero e non ingannevoli.

#### **4.2.2.2. Termini e condizioni dei contratti**

Rientra nella politica della Società negoziare in buona fede e in modo trasparente con tutti i potenziali clienti e fornitori, nonché evitare di porre in essere trattative non giustificate e destinate a non concludersi.

Esclusivamente le persone legittimate ed autorizzate dalla Società alla conclusione di contratti commerciali, in base al sistema di deleghe e di procure, di volta in volta in vigore, potranno negoziare eventuali modifiche delle politiche dei prezzi ovvero ai termini e condizioni dei contratti conclusi dalla Società.

#### **4.2.2.3. Consulenti**

Il ricorso all'attività professionale di Consulenti dovrà essere motivato, a cura del soggetto proponente, con l'indicazione per iscritto delle ragioni specifiche della proposta e della natura delle prestazioni che a questi ultimi verranno richieste.

La scelta del Consulente deve rigorosamente avvenire a favore di persone che, per la loro comprovata serietà e preparazione professionale, siano in grado di adempiere nel migliore dei modi all'incarico affidato.

Il pagamento del corrispettivo al Consulente dovrà essere effettuato sulla base di una dettagliata esposizione delle attività da quest'ultimo svolte, in modo che sia consentita la verifica della effettività e del valore delle prestazioni rese. La remunerazione al Consulente deve essere commisurata a quella normalmente praticata per prestazioni di analogo contenuto e qualità.

In ogni contratto stipulato con Consulenti dovrà essere formalizzato, a pena di risoluzione del contratto e di risarcimento di tutti i danni provocati, l'impegno da parte del Consulente ad uniformarsi a tutti i principi del presente Codice Etico e a rispettare tutte le norme di legge.

E' vietata ogni forma di raccomandazione o di pressione sugli organi delle società competenti a scegliere i Consulenti o finalizzata ad orientare la decisione di questi ultimi in maniera difforme dagli interessi aziendali. Ogni comportamento contrario deve ritenersi in contrasto con gli interessi aziendali.

#### **4.2.2.4. Utilizzo di informazioni riservate**

Se un dipendente o Collaboratore di *Computer Sciences Italia srl* viene a conoscenza di informazioni confidenziali, che non sono, quindi, di pubblico dominio e che riguardano *Computer Sciences Italia srl* o altre aziende, quali clienti o fornitori di *Computer Sciences Italia srl*:

- è suo dovere mantenere le informazioni riservate e non diffonderle a nessuno, se non su specifica richiesta e solo se autorizzato da *Computer Sciences Italia srl*;
- è suo dovere non comprare, vendere o consigliare l'acquisto o la vendita di titoli dell'azienda di cui ha acquisito informazioni riservate;
- è suo dovere assicurarsi che anche i suoi famigliari più stretti si conformino a queste regole.

Queste restrizioni valgono fintanto che le informazioni acquisite non siano rese pubbliche oppure cessino di essere materiale privato. Le informazioni non sono considerate di pubblico dominio sino a quando non vengono pubblicate e rese accessibili al pubblico.

#### **4.2.2.5. Pratiche anticoncorrenziali**

Nelle fasi negoziali con i clienti e fornitori, i dipendenti ed i Collaboratori dovranno fare attenzione ad evitare potenziali violazioni delle leggi in materia di antitrust e di concorrenza sleale.

La Società è libera di scegliere - sulla base di un proprio giudizio indipendente - i clienti con cui perfezionare accordi commerciali. Tuttavia questo diritto potrebbe trovare limitazioni nel caso in cui la Società abbia assunto dei vincoli mediante accordi precedentemente conclusi con terzi. Anche il solo dubbio circa la sussistenza di uno di questi vincoli deve indurre il dipendente e/o il collaboratore a consultare il Responsabile dell'Area aziendale Legal prima di intraprendere qualsiasi discussione con il cliente riguardante reali o potenziali concorrenti.

#### **4.2.2.6. Divieto di tangenti**

E' politica della Società assicurarsi che le fasi decisionali in ordine all'affidamento di forniture, appalti, subappalti o incarichi professionali siano caratterizzate da oggettività di giudizio e da assoluta conformità a leggi e regolamenti.

E' fatto divieto ai Soggetti destinatari di offrire od accettare tangenti; è vietata la maggiorazione, in forma diretta od indiretta, dei corrispettivi contrattuali applicati dai fornitori e/o dai Consulenti ovvero pattuiti con clienti della Società, inclusa la Pubblica Amministrazione, al fine di occultare tangenti per tali intendendosi qualunque importo, utilità, commissione, vantaggio, regalo, valore o compenso di qualunque tipo offerto, direttamente o indirettamente, allo scopo di influenzare decisioni commerciali, ottenere l'aggiudicazione di contratti o altri trattamenti di favore.

#### **4.2.2.7. Spese di rappresentanza**

La Società effettua spese di rappresentanza solo se autorizzate e comunque contenute. Di massima le spese di rappresentanza sono riferite ad attività di marketing.

### **4.2.3. Trasparenza nelle informazioni**

#### **4.2.3.1. Registrazione delle operazioni**

È principio fondamentale per *Computer Sciences Italia srl* che vi sia l'opportuna preventiva approvazione e registrazione di ogni azione od operazione effettuata in modo da consentire la verifica del processo di decisione.

Per ogni operazione dovrà essere predisposto adeguato supporto documentale che consenta di procedere ai controlli che attestino le motivazioni e le caratteristiche dell'operazione e individuino chi ha autorizzato, registrato, effettuato, verificato l'operazione stessa.

#### **4.2.3.2. Dati, Comunicazioni e Reports**

Tutti i dipendenti e i Collaboratori di *Computer Sciences Italia srl* sono responsabili della preparazione di tutta la documentazione relativa alle attività di business di *Computer Sciences Italia srl* nel modo più completo, onesto e accurato possibile.

Questa documentazione include rapportini, presenze, note spese, registrazioni contabili, risultati di test e report sullo stato avanzamento lavori, stime dei costi, proposte di contratto e presentazioni ai clienti, al pubblico o al management di *Computer Sciences Italia srl*.

Inoltre qualsiasi comunicazione, scritta o orale, fatta da qualunque dipendente, Collaboratore di *Computer Sciences Italia srl* o da chiunque rappresenti *Computer Sciences Italia srl* nella conduzione di affari dovrà basarsi su fatti, essere documentata e verificabile.

#### **4.2.3.3. Correttezza contabile**

I sistemi interni contabili, i risultati finanziari e le registrazioni contabili della Società devono rispecchiare, fedelmente e con ragionevole dettaglio, le operazioni effettuate, la relativa posizione finanziaria e le transazioni sottostanti, così come dovranno registrare correttamente la dismissione di beni ed attività patrimoniali. La contabilità interna dovrà essere coerente alle politiche di contabilità e finanza stabilite dalla Società e, comunque, rispettare i principi di contabilità generalmente accettati. Tutte le poste all'attivo ed al passivo della Società devono essere correttamente riportate nei libri contabili della Società.

#### **4.2.3.4. Rapporti con i revisori, i legali ed altri professionisti esterni**

Periodicamente, ai revisori della Società, agli avvocati ed ai professionisti esterni indipendenti potrà essere conferito mandato al fine di accertare la situazione legale, contabile e/o finanziaria della Società (ad esempio, in occasione di operazioni straordinarie o *audit* che si rendessero a qualsiasi titolo necessarie). I dipendenti, Collaboratori e/o Consulenti coinvolti in tali revisioni devono adottare un comportamento corretto e fornire ai rappresentanti della Società informazioni accurate e rispondenti al vero.

### **4.2.4. Altri obblighi di dipendenti e Collaboratori**

#### **4.2.4.1. Criteri di condotta etica e rispetto dei Protocolli e Policies**

Ogni dipendente e Collaboratore della Società è tenuto a svolgere la propria attività in modo responsabile, onesto e diligente, in conformità con la legge, con i Protocolli, le Policies aziendali in vigore e con le direttive stabilite dalla Società.

#### **4.2.4.2. Conflitto di Interessi**

Ogni dipendente e Collaboratore di *Computer Sciences Italia srl* deve fare attenzione ad evitare situazioni che potrebbero implicare un conflitto di interessi o che potrebbero apparire discutibili per gli altri.

In generale, ci sono due aree principali da tenere in considerazione:

- dare o ricevere qualunque cosa che possa influenzare chi riceve tale cosa o dare ad altri l'impressione che il ricevente potrebbe essere influenzato da ciò che gli viene offerto (per esempio offrire o accettare bustarelle, tangenti, pagamenti illegali o regalie);
- prendere parte ad attività che sono in conflitto o sembrano essere in conflitto con le responsabilità del dipendente nell'ambito di *Computer Sciences Italia srl*.

I dipendenti di *Computer Sciences Italia srl*, i loro familiari più stretti o i loro soci in attività di business devono evitare azioni che possano apparire in conflitto di interesse con le attività di *Computer Sciences Italia srl*, inclusa qualsiasi relazione finanziaria, di business o altro con fornitori, clienti o competitors, svolta al di fuori di *Computer Sciences Italia srl*.

Attività che possono sembrare in conflitto con quelle di *Computer Sciences Italia srl* sono, ad esempio, fare parte del consiglio di amministrazione di una società fornitrice o competitor di *Computer Sciences Italia srl*, fornire consulenza o lavorare per una società competitor o fornitrice.

#### **4.2.4.3. Protezione dei beni di Computer Sciences Italia srl e dei suoi clienti**

I dipendenti e Collaboratori di *Computer Sciences Italia srl* hanno l'obbligo di proteggere da perdita, furto e abuso, tutti i dati, comprese le informazioni che appartengono a *Computer Sciences Italia srl* e ai suoi clienti, i beni e le risorse finanziarie di *Computer Sciences Italia srl* e dei suoi clienti che sono stati affidati loro.

I beni aziendali, specialmente le attrezzature, i telefoni, i sistemi informativi interni, i database, i segreti commerciali e le altre informazioni confidenziali devono essere usate per finalità connesse all'esercizio della specifica attività lavorativa. I dipendenti non devono effettuare attività per conto proprio o di terzi durante l'orario di lavoro e - per l'esercizio di tali attività - non sono, pertanto, legittimati, né autorizzati ad utilizzare le dotazioni aziendali.

L'utilizzo degli strumenti informatici di lavoro da parte dei dipendenti deve essere pertanto conforme alle Procedure interne della Società ed alle leggi applicabili. I dipendenti non devono usare questi strumenti in maniera tale da danneggiare o offendere terzi.

Tutte le informazioni trattate o trasmesse elettronicamente sono da considerarsi proprietà delle Società e possono essere trasmesse esclusivamente per finalità connesse all'attività lavorativa. Le informazioni private e confidenziali delle Società devono essere adeguatamente identificate come tali.

Nessun dipendente di *Computer Sciences Italia srl* può divulgare informazioni a persone non autorizzate.

#### **4.2.4.4. Vantaggi personali in Computer Sciences Italia srl**

I dipendenti e Collaboratori di *Computer Sciences Italia srl* non devono:

- sfruttare a proprio vantaggio personale qualunque opportunità di cui sono venuti a conoscenza tramite l'uso di beni e informazioni appartenenti a *Computer Sciences Italia srl* o tramite la posizione ricoperta all'interno della Società;
- utilizzare beni o informazioni appartenenti a *Computer Sciences Italia srl* o sfruttare il ruolo ricoperto all'interno della Società per ottenere un guadagno personale;
- svolgere attività in competizione con *Computer Sciences Italia srl*.

#### **4.2.5. Pari opportunità/divieto di discriminazioni**

E' politica della Società garantire a tutti pari opportunità di accesso e progressione professionale, nonché intraprendere azioni positive finalizzate ad avere una forza lavoro che sia rappresentativa delle diverse provenienze sociali. Ciò significa che ogni decisione afferente la valutazione delle risorse umane sarà assunta in maniera non discriminatoria. La Società non ritiene ammissibili, né tollererà forme di discriminazioni basate sulla razza, colore, sesso, età, religione, condizione fisica, stato civile, orientamenti sessuali, cittadinanza, origine etnica o qualunque altra discriminazione contraria alla legge.

La Società non porrà in essere, né tollererà alcuna forma di ritorsione nei confronti dei dipendenti che abbiano lamentato modalità di discriminazione o di molestia, né nei confronti dei lavoratori che abbiano fornito notizie in merito.

#### **4.2.6. Rapporti con la Pubblica Amministrazione**

*Computer Sciences Italia srl* ha come principio cardine della propria attività quello di intraprendere rapporti con la Pubblica Amministrazione caratterizzati dalla massima trasparenza e dalla completa adesione alle disposizioni di legge al fine di assicurare la miglior qualità tecnica dei servizi e di applicare le migliori condizioni economiche.

##### **4.2.6.1. Regalie, pagamenti illeciti, doni o offerte di denaro verso la Pubblica Amministrazione**

Non è assolutamente consentito offrire denaro o doni a dirigenti, funzionari, o dipendenti della Pubblica Amministrazione o a loro parenti, sia italiani che di altri paesi, salvo che si tratti di doni o utilità d'uso di modico valore.

Si considerano atti di corruzione, sia i pagamenti illeciti fatti direttamente da dipendenti italiani, sia i pagamenti fatti tramite persone che agiscono per conto di *Computer Sciences Italia srl*, sia in Italia che all'estero.

È proibito a tutti i dipendenti e Dirigenti di *Computer Sciences Italia srl*, offrire o accettare, direttamente o tramite terzi, qualsiasi oggetto, servizio, prestazione o favore di valore, ricevuto per ottenere un trattamento più favorevole in relazione a qualsiasi rapporto intrattenuto con la Pubblica Amministrazione.

##### **4.2.6.2. Influenza negli affari con la Pubblica Amministrazione**

Quando è in corso una attività commerciale e/o trattativa d'affari, richiesta o rapporto con la Pubblica Amministrazione, non si deve cercare di influenzare impropriamente le decisioni della controparte, comprese quelle dei funzionari che trattano o prendono decisioni per conto della Pubblica Amministrazione.

Nel rapportarsi con la Pubblica Amministrazione o nel partecipare a bandi ad evidenza pubblica, i dipendenti, ed i terzi sono tenuti ad essere particolarmente attenti alla confidenzialità, all'integrità, alla veridicità e completezza della documentazione presentata alla Pubblica Amministrazione ed al rispetto delle norme pubblicistiche.

Nel caso di effettuazione di una gara con la Pubblica Amministrazione, si dovrà operare nel rispetto della legge e della corretta pratica commerciale.

Nel caso si utilizzi un consulente o un soggetto terzo per essere rappresentato nei rapporti verso la Pubblica Amministrazione, nei confronti del consulente e del suo personale o nei confronti del soggetto terzo saranno applicate le stesse direttive valide anche per i dipendenti di *Computer Sciences Italia srl*. Comunque, la Società non dovrà farsi rappresentare da un consulente o soggetto terzo nel caso si configuri un conflitto di interessi.

Nel corso di una trattativa d'affari, richiesta o rapporto commerciale con la Pubblica Amministrazione non vanno assolutamente intraprese (direttamente o indirettamente) le seguenti azioni:

- esaminare o proporre opportunità di impiego e/o commerciali che possano avvantaggiare i dipendenti o funzionari della Pubblica Amministrazione a titolo personale;
- offrire danaro, regali, doni, omaggi, pagamenti illeciti, etc. o in alcun modo fornire promesse di favori di alcun tipo;
- sollecitare o ottenere informazioni riservate che possano compromettere l'integrità o la reputazione di CSC Computer Sciences Italia srl e/o della Pubblica Amministrazione.

#### **4.2.6.3. Forniture, appalti e subappalti**

Le forniture, gli appalti e i subappalti devono essere motivati da effettive esigenze aziendali e la scelta del fornitore deve, in ogni caso, essere effettuata tenendo esclusivamente conto di parametri tecnici, professionali ed economici.

La scelta del fornitore e la stipula del contratto di fornitura dovranno avvenire nel rispetto di tutte le norme di legge e delle regole in materia di appalto e subappalto, specie nel settore dei contratti ad evidenza pubblica.

In ogni contratto di fornitura dovrà essere formalizzato, a pena di risoluzione del contratto e di risarcimento di tutti i danni provocati, l'impegno da parte del fornitore ad uniformarsi a tutti i principi del presente Codice Etico e a rispettare tutte le norme di legge.

E' vietata ogni forma di raccomandazione o di pressione sugli organi competenti della Società finalizzata a scegliere i fornitori e/o finalizzata ad orientare la decisione di questi ultimi in maniera difforme dagli interessi aziendali.

#### **4.2.6.4. Assunzione di personale legato alla Pubblica Amministrazione**

*Computer Sciences Italia srl* ha attivato specifiche Policies che regolamentano l'assunzione di personale che direttamente o indirettamente possa essere collegabile con l'area della Pubblica Amministrazione. Si fa particolare riferimento ad ex impiegati della Pubblica Amministrazione (o loro parenti) che abbiano partecipato personalmente e attivamente a trattative d'affari, o ad avallare le richieste effettuate da *Computer Sciences Italia srl* ad entità proprie della Pubblica Amministrazione o che abbiano partecipato a verifiche di legge sull'operato della Società o che abbiano in corso attività istruttorie riguardo alla Società stessa.

#### **4.2.7. Finanziamento ai partiti politici**

*Computer Sciences Italia srl* può contribuire al finanziamento di partiti politici, comitati, organizzazioni pubbliche o candidati politici purché nel rispetto delle normative vigenti.

#### **4.2.8. Sicurezza sul lavoro ed igiene ambientale**

CSC Computer Sciences Italia srl ha approntato le misure necessarie per la protezione della salute e sicurezza sui luoghi di lavoro, comprese le attività di prevenzione dei rischi professionali, di informazione e formazione, nonché di pianificazione dell'organizzazione e dei mezzi necessari.

A tale proposito la Società si impegna:

- ad adottare le misure più opportune per evitare i rischi connessi allo svolgimento della propria attività ed a monitorare i rischi non eliminabili attraverso valutazioni periodiche e conseguenti piani di adeguato contrasto;
- ad adeguare il lavoro all'uomo, in particolare per quanto concerne la concezione dei posti di lavoro e la scelta delle attrezzature di lavoro e dei metodi di lavoro e di produzione, in particolare per attenuare il lavoro monotono e il lavoro ripetitivo e per ridurre gli effetti di questi lavori sulla salute;
- a tener conto del grado di evoluzione della tecnica e sostituire ciò che è pericoloso con ciò che non è pericoloso o che è meno pericoloso;
- a dare la priorità alle misure di protezione collettiva rispetto alle misure di protezione individuale;
- a impartire adeguate istruzioni ai lavoratori;
- a programmare la prevenzione in materia di salute e sicurezza sul lavoro, mirando ad un complesso coerente che integri nella medesima la tecnica, l'organizzazione del lavoro, le condizioni di lavoro, le relazioni sociali e l'influenza dei fattori dell'ambiente di lavoro.

Il personale di *Computer Sciences Italia srl*:

- contribuisce all'adempimento degli obblighi previsti per la tutela della salute e della sicurezza sul luogo di lavoro;
- si impegna a rispettare le istruzioni e le disposizioni impartite dal datore di lavoro ai Responsabili delle Aree Aziendali;
- partecipa ai corsi di formazione organizzati dal datore di lavoro;
- si impegna a sottoporsi ai controlli sanitari previsti dalla normativa e disposti dal medico competente.

#### **4.2.9. Antiriciclaggio e ricettazione**

*Computer Sciences Italia srl* ha come principio quello della massima trasparenza delle transazioni ed attua i dovuti controlli per contrastare il fenomeno del riciclaggio e della ricettazione. Nel perseguimento della massima trasparenza nelle transazioni commerciali *Computer Sciences Italia srl* attua i dovuti controlli nel rispetto dei seguenti principi:

- qualificazione dei nuovi fornitori;
- vaglio degli acquisti di nuovi beni e servizi;
- valutazione delle forniture;
- monitoraggio delle uscite finanziarie;
- registrazione degli incassi e della fatturazione attiva;
- compimento di accertamenti riguardo la gestione dell'IWO;
- sorveglianza dell'attività commerciale e di marketing.

#### **4.2.10. Criminalità informatica**

*CSC Computer Sciences Italia srl* ha come principio quello di contrastare fortemente la criminalità informatica.

Allo scopo, la Società ha posto in essere una serie di Procedure rivolte a garantire la limitazione d'accesso agli archivi informatici (software e dati) solo alle persone autorizzate, mantenendo inoltre la tracciabilità delle operazioni svolte.

*Computer Sciences Italia srl* ha posto in essere le Procedure e gli standard del gruppo di appartenenza per il mantenimento di alti livelli di sicurezza per quanto attiene la comunicazione attraverso le reti informatiche ed internet.

Il personale di *Computer Sciences Italia srl* mantiene un adeguato standard qualitativo di sicurezza per gli interventi da svolgere presso i sistemi informatici dei clienti nell'ambito e tenuto conto dei rapporti contrattuali con essi intrattenuti.

E' fatto divieto di utilizzare i sistemi informatici aziendali e dei clienti per scopi non attinenti strettamente il mandato operativo ricevuto.

In ogni momento lavorativo al personale è fatto obbligo di attenersi alle direttive ed alle Disposizioni aziendali emesse in materia.

#### **4.2.11. Comunicazione all'interno di Computer Sciences Italia srl**

*CSC Computer Sciences Italia srl* incoraggia la libera comunicazione tra i dipendenti a tutti i livelli.

A tal fine è stato predisposto un documento denominato *Policy sui flussi di comunicazione con l'Organismo di Vigilanza* che ciascun dipendente dovrà rispettare.

I Soggetti destinatari potranno comunque contattare l'Organismo di vigilanza e riferire eventuali dubbi, problemi o questioni relativi a tematiche rilevanti ai fini del Decreto (ad esempio contabilità, sicurezza, controllo di gestione e audit).

Se un Soggetto destinatario ha ragione di credere che si sia verificata o che possa verificarsi una violazione di questi standard di condotta o di qualunque altra procedura aziendale si avvarrà dei canali ad esso dedicati.

La Società non rivelerà, senza la debita autorizzazione, l'identità di un dipendente che abbia fatto una segnalazione a meno che la rivelazione della sua identità non possa essere evitata nel corso di un'indagine.

In nessun caso verrà intrapresa un'azione disciplinare nei confronti di un dipendente di *CSC Computer Sciences Italia srl* che abbia segnalato correttamente una sospetta infrazione.

Queste segnalazioni saranno trattate con la massima riservatezza nella maniera più coerente possibile con l'applicazione rigorosa e corretta del Codice Etico.

## 5. L'ORGANISMO DI VIGILANZA

### 5.1. IDENTIFICAZIONE DELL'ORGANISMO DI VIGILANZA

Gli artt. 6 e 7 del Decreto prevedono che l'ente possa essere esonerato dalla responsabilità connessa alla commissione dei reati indicati nel Decreto qualora l'organo dirigente abbia, fra l'altro:

- a) adottato il modello di organizzazione, gestione e controllo e lo abbia efficacemente attuato, e
- b) affidato il compito di vigilare sul funzionamento e sull'osservanza del modello di organizzazione, gestione e controllo e di curarne l'aggiornamento ad un organismo dell'ente dotato di autonomi poteri di iniziativa e controllo.

*Computer Sciences Italia srl* ha istituito l'Organismo di vigilanza e ha determinato i suoi poteri, responsabilità e compiti più oltre specificati.

La responsabilità degli aggiornamenti ed adeguamenti del Modello Organizzativo, nonostante l'istituzione dell'Organismo di vigilanza, è rimessa direttamente al Consiglio di Amministrazione di *Computer Sciences Italia srl*, sentite le considerazioni e le proposte dell'Organismo di vigilanza.

A riguardo, si precisa che il Consiglio di Amministrazione, pur con l'istituzione dell'Organismo di vigilanza, mantiene invariate tutte le attribuzioni e le responsabilità previste dalla legge, dal citato Decreto e dal codice civile in generale, alle quali si aggiunge quella relativa all'adozione, al rispetto delle disposizioni e all'efficacia del Modello Organizzativo, nonché all'istituzione dell'Organismo di vigilanza.

Nel contempo, le attività necessarie e strumentali all'attuazione delle disposizioni del Modello Organizzativo sono poste in essere direttamente dalle Funzioni aziendali, sotto la responsabilità del Responsabile di ogni Funzione aziendale e del Responsabile di ogni Area aziendale.

### 5.2. REQUISITI DELL'ORGANISMO DI VIGILANZA

L'Organismo di vigilanza di *Computer Sciences Italia srl*:

- o è dotato di requisiti di indipendenza e autonomia;
- o possiede adeguata professionalità;
- o è dotato di autonomi poteri di iniziativa e controllo;
- o possiede il requisito della continuità di azione.

#### 5.2.1. Indipendenza e autonomia

La necessaria autonomia dei membri dell'Organismo di vigilanza di *Computer Sciences Italia srl* è garantita in ragione della:

- collocazione in posizione gerarchica di vertice in *Computer Sciences Italia srl* assicurata dal rapporto in modo diretto ed esclusivo al Consiglio di Amministrazione;
- emanazione in autonomia di un proprio Regolamento messo a conoscenza del Consiglio di Amministrazione;
- dotazione di adeguate risorse finanziarie che vengono utilizzate per ogni esigenza necessaria al corretto svolgimento delle attività proprie dell'Organismo di vigilanza. Del fondo avuto in dotazione l'Organismo di vigilanza dovrà rendere conto con cadenza annuale al Consiglio di Amministrazione chiedendo, se del caso, opportune integrazioni dello stesso;
- assenza di soggezione, in forza di tale qualità e nell'ambito di svolgimento della propria funzione, al potere gerarchico e disciplinare di alcun altro organo o funzione societaria;
- assenza di incarichi operativi nella Società;
- assenza di conflitti di interessi e di legami di parentela con i vertici della Società;

- presenza dei requisiti di onorabilità di cui alle disposizioni in tema di cause di ineleggibilità e decadenza previste per l'elezione alla carica di sindaco nelle società per azioni di cui all'art. 2399, 1° comma del codice civile.

### **5.2.2. Professionalità**

L'Organismo di vigilanza è composto da professionisti esterni dotati di specifiche competenze tecniche nel campo delle Procedure di Controllo interno, della valutazione dei rischi e delle misure per il loro contenimento, nonché da esperti di materie giuridiche rilevanti ai fini del Decreto.

L'Organismo di vigilanza, nello svolgimento della propria attività, inoltre:

- si avvale del supporto delle Aree aziendali e delle Funzioni aziendali della Società;
- si può avvalere di risorse esterne a *Computer Sciences Italia srl* (es.: servizi professionali e/o di consulenza specialistica).

### **5.2.3. Autonomia nei poteri di iniziativa e controllo**

L'Organismo di vigilanza di *Computer Sciences Italia srl* definisce e svolge in modo autonomo le attività di competenza, comprese le attività proprie di controllo.

Le regole di funzionamento interno dell'Organismo di vigilanza sono definite dallo stesso nel proprio Regolamento.

Come indicato dalle Linee Guida di Confindustria infatti, mentre il Modello Organizzativo (e sue eventuali modifiche) viene approvato dal Consiglio di Amministrazione, il Regolamento rappresenta l'autoregolamentazione operativa dell'Organismo di vigilanza che, appunto, è approvato in piena autonomia dall'Organismo di vigilanza stesso.

### **5.2.4. Continuità di azione**

I membri dell'Organismo di vigilanza garantiscono un impegno costante nell'attività di vigilanza del Modello Organizzativo. Essi, pur essendo soggetti esterni alla Società, sono a conoscenza della struttura e dell'attività di *Computer Sciences Italia srl*. La continuità d'azione è garantita anche dalla predisposizione di canali di raccordo con la Società.

L'Organismo di vigilanza infatti è coadiuvato e supportato attivamente dai Responsabili delle Aree aziendali e dai Responsabili di Funzione.

### **5.2.5. Acquisizione delle informazioni**

L'acquisizione delle informazioni necessarie all'operatività dell'Organismo di vigilanza viene assicurata, tra l'altro,

- attraverso i flussi informativi verso l'Organismo di vigilanza definiti dal Regolamento e dalla specifico documento *Policy sui flussi di comunicazione con l'Organismo di Vigilanza* e dal Modello Organizzativo stesso;
- attraverso le richieste dell'Organismo di vigilanza stesso verso le strutture interessate;
- attraverso le interviste programmate al personale interno e le verifiche documentali;
- attraverso la partecipazione di uno dei membri dell'Organismo di vigilanza ai momenti decisionali aziendali, laddove vengano trattati temi inerenti i rischi di reato di cui al Decreto.

### **5.2.6. Rapporto agli Organi sociali**

L'Organismo di vigilanza riporta direttamente al Consiglio di Amministrazione.

## **5.3. NOMINA DEI MEMBRI DELL'ORGANISMO DI VIGILANZA**

*Computer Sciences Italia srl* ha costituito l'Organismo di vigilanza deputato alla vigilanza e al controllo del presente Modello Organizzativo. Attualmente i membri dell'Organismo di vigilanza, nominati con delibera del Consiglio di Amministrazione del 16 dicembre 2008, sono:

- [..omissis..], dottore commercialista e revisore contabile;
- [..omissis..], dottore commercialista e revisore contabile;
- [..omissis..], avvocato.

Il dott. [...omissis...] è stato nominato presidente dell'Organismo di vigilanza.

I membri dell'Organismo di vigilanza sono stati nominati tra soggetti esterni a *Computer Sciences Italia srl* e sono in possesso dei requisiti indicati dal Decreto e dalle disposizioni in tema di cause di ineleggibilità e decadenza previste per l'elezione alla carica di sindaco nelle società per azioni di cui all'art. 2399, 1° comma del codice civile.

L'Organismo di vigilanza rimarrà in carica 3 anni e alla naturale scadenza potrà essere consensualmente riconfermato.

Oltre a quanto esplicitato nei paragrafi precedenti, la nomina a membro dell'Organismo di vigilanza comporta:

1. che ciascun membro dell'Organismo di vigilanza è tenuto al rispetto di quanto indicato nel Modello Organizzativo in vigore presso *Computer Sciences Italia srl* dal momento della nomina e per tutta la durata del mandato;
2. che ciascun membro dell'Organismo di vigilanza è tenuto al segreto riguardo notizie e informazioni acquisite nell'esercizio delle proprie funzioni. I membri dell'Organismo di vigilanza assicurano la riservatezza delle informazioni acquisite, in particolare, se relative a presunte violazioni del Modello Organizzativo; inoltre, si astengono dal ricercare ed utilizzare informazioni riservate per scopi diversi da quelli previsti dal Decreto, o in ogni caso per fini non conformi ai loro compiti.

Gli obblighi dell'Organismo di vigilanza sono correlati al Modello Organizzativo in vigore durante il periodo di nomina.

## **5.4. RINUNCIA, REVOCA, E SANZIONI**

Ciascuno dei membri dell'Organismo di vigilanza può rinunciare all'incarico motivando la propria decisione.

Nel pieno rispetto dei principi etici e comportamentali che infondono il Modello Organizzativo, è altresì fatto obbligo a ciascuno dei membri dell'Organismo di vigilanza di presentare le dimissioni dall'incarico nel caso in cui, a qualunque titolo, sopraggiungano cause di incompatibilità e/o di impossibilità per l'effettuazione delle attività e l'assunzione delle proprie responsabilità e/o, comunque, in caso di conflitto di interessi.

Il Consiglio di Amministrazione può deliberare la revoca dell'incarico all'OdV soltanto per giustificati motivi.

A tale riguardo, per giustificati motivi dovranno intendersi:

- l'interdizione o l'inabilitazione, ovvero una grave infermità che renda uno dei componenti dell'Organismo di vigilanza inidoneo a svolgere le proprie funzioni di vigilanza, o un'infermità che, comunque, comporti l'assenza per un periodo superiore a sei mesi;
- un grave inadempimento dei propri doveri così come definiti nel Modello Organizzativo;
- una sentenza di condanna passata in giudicato, a carico di uno dei membri dell'Organismo di vigilanza per aver personalmente commesso uno dei reati previsti dal Decreto;
- una sentenza di condanna passata in giudicato, a carico di uno dei componenti dell'Organismo di vigilanza ad una pena che comporta l'interdizione, anche temporanea, dai pubblici uffici, ovvero l'interdizione temporanea dagli uffici direttivi delle persone giuridiche e delle imprese;
- l'assenza ingiustificata di un componente dell'Organismo di vigilanza a tre riunioni nell'anno, anche non consecutive, e la mancata collaborazione ai programmi dell'Organismo di vigilanza.

L'Organismo di vigilanza stesso può chiedere al Consiglio di Amministrazione la revoca di uno dei suoi membri per fondati motivi o per evidente conflitto di interesse.

Ogni variazione nel tempo della composizione dell'Organismo di vigilanza e la conseguente approvazione delle modifiche al Modello Organizzativo, deve essere deliberata dal Consiglio di Amministrazione, sentito il parere non vincolante dell'Organismo di vigilanza stesso.

Tale parere deve essere riportato nel verbale della relativa riunione del Consiglio di Amministrazione.

## 5.5. FUNZIONI, ATTIVITÀ E POTERI DELL'ORGANISMO DI VIGILANZA

L'Organismo di vigilanza è dotato dell'autorità e dei poteri per vigilare in autonomia sul funzionamento e sull'osservanza del Modello Organizzativo, per garantire l'effettività e la razionalità del Modello Organizzativo, per vagliare l'adeguatezza del medesimo.

Di seguito, un'elencazione delle funzioni, poteri ed attività attribuite all'Organismo di vigilanza anche sulla base delle indicazioni contenute negli artt. 6 e 7 del Decreto. Maggiori dettagli riguardo il funzionamento dell'Organismo di vigilanza saranno indicati nel Regolamento predisposto dall'Organismo di vigilanza stesso. L'Organismo di vigilanza:

- vigila periodicamente sull'effettività del Modello Organizzativo, che si sostanzia nella verifica della coerenza tra i comportamenti concretamente attuati in azienda e quanto previsto dalle disposizioni contenute nel Modello Organizzativo;
- valuta l'adeguatezza del Modello Organizzativo: ossia della sua reale (e non meramente formale) capacità di prevenire, in linea di massima, i comportamenti non voluti;
- analizza periodicamente il mantenimento nel tempo dei requisiti di solidità e funzionalità del Modello Organizzativo;
- attiva periodicamente le Procedure di controllo e conduce ricognizioni dell'attività aziendale ai fini dell'aggiornamento della mappatura delle aree a rischio-reato;
- cura l'aggiornamento necessario del Modello Organizzativo nell'ipotesi in cui le analisi operate rendano necessario effettuare correzioni ed adeguamenti.

Tale aggiornamento si divide in due fasi distinte ed integrate:

- presentazione di proposte di adeguamento del Modello Organizzativo verso il Consiglio di Amministrazione. A seconda della tipologia e della portata degli interventi, le proposte di adeguamento potranno essere dirette anche verso le specifiche Funzioni aziendali;
- *follow-up*, ovvero verifica sistematica e compiuta dell'attuazione e dell'effettiva funzionalità delle soluzioni proposte e definite;
- gestisce, approfondisce e verifica la normativa oggetto del Codice Etico al fine di adeguarlo all'evoluzione legislativa e dei contratti collettivi;
- promuove le iniziative per la diffusione della conoscenza del Modello Organizzativo, nonché per la formazione del personale e la sensibilizzazione dello stesso all'osservanza dei principi contenuti nel Modello Organizzativo, di concerto con l'Area aziendale HR;
- è costantemente, tempestivamente e sistematicamente informato di tutti i fatti, operazioni ed accadimenti riguardanti la gestione ed il governo di *Computer Sciences Italia srl* rilevanti ai fini del Decreto;
- ha la facoltà di chiedere e/o assegnare a soggetti terzi, in possesso delle competenze specifiche necessarie per la migliore esecuzione dell'incarico, compiti di natura meramente tecnica;
- può procedere ad interventi di controllo in qualsiasi momento, nell'ambito della propria autonomia e discrezionalità;
- può accedere senza limitazioni alle informazioni aziendali per svolgere le attività allo stesso delegate;
- può consultare documenti, accedere ai sistemi informativi aziendali per acquisire dati e/o informazioni necessari alle attività di analisi, verificare l'operato delle funzioni nonché effettuare interviste alle persone preposte nelle singole fasi di un determinato processo a rischio;
- effettua controlli sul comportamento degli utenti degli strumenti informatici avvalendosi della collaborazione della funzione del MSS, a cui l'Organismo di vigilanza periodicamente chiederà informazioni riguardo la sussistenza o meno di eventuali problematiche nell'utilizzazione degli strumenti informatici da parte degli utenti. Le verifiche compiute dall'Organismo di vigilanza saranno condotte sempre nel rispetto del diritto di riservatezza

degli utenti e dei titolari dei dati trattati, anche rispetto ai rapporti esterni tenuti attraverso gli strumenti informatici;

- partecipa per mezzo di un proprio membro, alle riunioni del Consiglio di amministrazione o qualsiasi altro comitato, qualora vengano trattati temi inerenti i rischi di reato ai sensi del Decreto;
- stende il programma annuale di attività;
- attua il programma annuale di attività;
- valuta i risultati delle verifiche effettuate o delle informazioni ricevute ed il loro impatto sul Modello Organizzativo.

Lo svolgimento delle attività sopra indicate è affiancata e coadiuvata:

- dal rispetto da parte dei Soggetti destinatari delle regole sui flussi informativi verso l'Organismo di vigilanza nonché dell'obbligo di dare riscontro a specifiche richieste informative formulate dall'OdV, come previsto dal Modello Organizzativo e dal documento *Policy sui flussi di comunicazione con l'Organismo di vigilanza*;
- dal rispetto da parte dell'OdV dell'obbligo di riporto scritto e orale verso il Consiglio di Amministrazione, nonché dell'obbligo di dare riscontro a specifiche richieste informative del Consiglio di Amministrazione come previsto dal Modello Organizzativo e dal documento *Policy sui flussi di comunicazione con l'Organismo di vigilanza*.

In caso di violazioni direttamente riscontrate o segnalate l'OdV:

- verifica, controlla e valuta i casi di violazione delle norme aziendali, provvedendo, nel caso di infrazioni, alle misure opportune, in collaborazione con i responsabili aziendali competenti nel rispetto delle leggi, dei regolamenti e dei contratti collettivi;
- conduce approfondimenti per l'accertamento di presunte violazioni delle prescrizioni del presente Modello Organizzativo;
- segnala, al Consiglio di Amministrazione, al Collegio Sindacale e all'Area aziendale HR la notizia di violazione del Modello Organizzativo;
- monitora, di concerto con il Consiglio di Amministrazione e con l'Area aziendale HR, l'applicazione delle sanzioni disciplinari;
- tutela i soggetti che segnalano comportamenti non conformi al Codice Etico e alle disposizioni di cui al Modello Organizzativo, attraverso iniziative concordate con l'Area aziendale HR.

Ai fini della gestione e prevenzione del rischio di violazioni attinenti la normativa di salute e sicurezza sul lavoro, l'Organismo di vigilanza esegue un controllo dell'efficienza ed efficacia delle procedure rilevanti ai sensi del Decreto del tutto indipendente e differenziata dall'attività di controllo tecnico-operativa di competenza del RSPP.

## **5.6. OBBLIGHI DI INFORMAZIONE VERSO L'ORGANISMO DI VIGILANZA**

Per permettere il corretto funzionamento dell'Organismo di vigilanza, i Soggetti destinatari sono tenuti al rispetto dei flussi informativi previsti:

1. dal presente Modello Organizzativo;
2. dal documento *Policy sui flussi di comunicazione con l'Organismo di Vigilanza*;
3. dal documento annuale redatto dall'Organismo di vigilanza relativamente a specifiche informazioni da trasmettere;
4. dalla Mappatura dei Rischi.

Il flusso informativo verso l'Organismo di vigilanza è un adempimento obbligatorio a carico di tutti i Soggetti destinatari nell'ambito delle attività poste in essere per la prevenzione dei reati previsti dal Decreto.

A tal fine, all'Organismo di vigilanza devono essere trasmesse le informazioni aventi per oggetto i comportamenti non conformi a quanto previsto nella Parte Speciale e nella Mappatura dei Rischi, nonché le informazioni su tutti quegli eventi che siano in qualsiasi modo attinenti alle attività a rischio-reato.

L'Organismo di vigilanza deve essere tempestivamente informato di ogni cambiamento in essere o pianificato, inerente e/o avente ad oggetto il Modello Organizzativo e/o la struttura/assetto societario in generale rilevante ai fini del Decreto.

L'Organismo di vigilanza deve essere informato, mediante apposite segnalazioni da parte dei Soggetti destinatari, in merito ad eventi che potrebbero ingenerare responsabilità per *Computer Sciences Italia srl* ai sensi del Decreto.

Si riportano di seguito alcune prescrizioni di carattere generale che riguardano i flussi di comunicazione verso l'Organismo di vigilanza.

- Devono essere comunicate all'Organismo di vigilanza tutte le deleghe e/o procure conferite ai vari responsabili e/o soggetti che operano in una delle attività definite a rischio-reato e le modifiche delle stesse.
- Devono essere raccolte da ciascun Responsabile dell'Area aziendale tutte le eventuali segnalazioni relative alla commissione, o al ragionevole pericolo di commissione, dei reati contemplati dal Decreto; o comunque a comportamenti in generale non in linea con i principi contenuti nel Codice Etico e con le regole di comportamento di cui al presente Modello Organizzativo.
- I Responsabili di Area aziendale e i Responsabili di Funzione aziendale devono: (i) attestare annualmente all'Organismo di vigilanza la corrispondenza dei Protocolli/Controlli preventivi indicati nella Mappatura dei Rischi con la realtà operativa in essere nonché, (ii) segnalare tempestivamente gravi anomalie nel funzionamento del Modello Organizzativo o violazioni di prescrizioni dello stesso.
- Ciascun dipendente di *Computer Sciences Italia srl* deve segnalare la violazione (o anche la presunta violazione) del presente Modello Organizzativo, contattando il proprio diretto superiore gerarchico e/o l'Organismo di vigilanza. Con disposizione dell'Organismo di vigilanza sono istituiti canali informativi dedicati per facilitare il flusso di segnalazioni e informazioni officiose, che garantiscano in ogni caso la riservatezza della segnalazione.
- I Consulenti, i Collaboratori e i partners commerciali e le terze parti, per quanto riguarda la loro attività svolta con *Computer Sciences Italia srl*, effettuano la segnalazione direttamente all'Organismo di vigilanza mediante "canali informativi dedicati" da definire contrattualmente.
- L'Organismo di vigilanza deve ricevere le notizie relative ai procedimenti disciplinari azionati anche in relazione a notizia di violazione del Modello Organizzativo e alle sanzioni irrogate (ivi compresi i provvedimenti assunti verso i dipendenti), come pure notizie circa l'andamento di tali procedimenti.
- L'Organismo di vigilanza è tenuto a valutare correttamente le segnalazioni ricevute e le attività da porre in essere. Gli eventuali provvedimenti conseguenti dovranno essere definiti e applicati in conformità a quanto previsto in ordine al Sistema disciplinare definito.
- L'Organismo di vigilanza può non prendere in considerazione eventuali segnalazioni anonime.

È impegno preciso dell'Organismo di vigilanza di *Computer Sciences Italia srl*, assicurare la necessaria e dovuta riservatezza e confidenzialità riguardo all'identità delle persone che effettuano le segnalazioni, al fine di evitare qualsiasi forma di ritorsione, discriminazione o penalizzazione.

Nel caso in cui l'Organismo di vigilanza riceva notizie e/o informazioni false, fornite in mala fede, e/o con dolo sarà dovere dell'Organismo di vigilanza segnalare l'accaduto ai soggetti titolari del potere di porre in essere gli eventuali provvedimenti conseguenti.

In ogni caso, in aggiunta ai suddetti obblighi di informazione, e' fatto obbligo in capo a qualunque Funzione aziendale e a qualsiasi dipendente e/o componente degli organi sociali, di fornire tutte le informazioni necessarie a fronte di richieste da parte dell'Organismo di vigilanza, o al verificarsi di eventi o circostanze rilevanti ai fini nello svolgimento delle attività dell'Organismo di vigilanza.

Sono, naturalmente, fatti salvi tutti gli obblighi di legge per la tutela dei diritti della Società e delle persone.

### **5.6.1. Gestione delle informazioni**

Tutte le informazioni, segnalazioni, report, etc. sono opportunamente gestiti e conservati dall'Organismo di vigilanza in un apposito data base, tool informatico e/o anche cartaceo.

Per l'accesso a tali dati/informazioni sono previsti criteri e condizioni di accesso riservati.

Tutti i dati archiviati e custoditi dall'Organismo di vigilanza, possono essere messi a disposizione di soggetti esterni all'Organismo di vigilanza solo previa debita autorizzazione scritta di quest'ultimo.

## **5.7. RIPORTO DELL'ORGANISMO DI VIGILANZA VERSO IL CONSIGLIO DI AMMINISTRAZIONE**

L'Organismo di vigilanza di *Computer Sciences Italia srl* riferisce formalmente in merito:

- A. all'attuazione del Modello Organizzativo;
- B. ad eventuali aspetti critici;
- C. all'esito delle attività di verifica svolte nell'esercizio dei compiti assegnati.

A tal fine, l'Organismo di vigilanza:

- formula le sue proposte al Consiglio di Amministrazione per gli eventuali aggiornamenti, modifiche ed adeguamenti del Modello Organizzativo che dovessero essere necessarie a seguito: (i) di violazioni delle prescrizioni di cui al Modello Organizzativo; (ii) di significative modificazioni dell'assetto interno della Società e (iii) di modifiche normative;
- segnala al Consiglio di Amministrazione ogni violazione accertata del Modello Organizzativo che possa comportare l'insorgere di una responsabilità in capo alla Società per gli opportuni provvedimenti.

L'Organismo di vigilanza predisponde semestralmente una relazione per il Consiglio di Amministrazione avente ad oggetto gli esiti della sua attività. La relazione predisposta in favore degli amministratori sarà poi resa disponibile su richiesta al Collegio Sindacale. L'Organismo di vigilanza potrà predisporre altre specifiche relazioni ricorrendone la necessità.

All'Organismo di vigilanza potrà essere richiesto di riferire in qualsiasi momento, da parte dei suddetti organi, come pure l'Organismo di vigilanza stesso potrà riferire, in merito a situazioni specifiche e/o ritenute pregiudizievoli.

## 6. IL SISTEMA DISCIPLINARE

### 6.1. FINALITÀ DEL SISTEMA DISCIPLINARE

Ai sensi degli artt. 6 e 7 del Decreto, *Computer Sciences Italia srl* deve definire e porre in essere "un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello".

Questo è un aspetto fondamentale del Modello Organizzativo, il quale deve prevedere l'esistenza di adeguate sanzioni per la violazione delle regole ivi definite al fine della prevenzione dei reati.

Infatti, la previsione di sanzioni, debitamente commisurate alla violazione e dotate di "meccanismi di deterrenza", applicabili in caso di violazione del Modello Organizzativo, ha lo scopo di contribuire da un lato all'efficacia del Modello Organizzativo stesso, e dall'altro, all'efficacia dell'azione di controllo effettuata dall'Organismo di vigilanza.

Tali violazioni infatti incrinano il rapporto improntato in termini di trasparenza, correttezza, lealtà e integrità instaurato tra *Computer Sciences Italia srl* e i Soggetti destinatari; di conseguenza, saranno poste in essere opportune azioni a carico dei soggetti interessati.

Il sistema disciplinare definito, per i fini del presente Modello Organizzativo, è parte integrante delle obbligazioni contrattuali assunte dai Soggetti destinatari.

È utile sottolineare che l'applicazione delle sanzioni previste, è svincolata e del tutto autonoma rispetto allo svolgimento e all'esito di un eventuale procedimento penale eventualmente avviato dall'autorità giudiziaria competente.

Pertanto, il giudizio promosso da *Computer Sciences Italia srl* potrebbe non coincidere con quello espresso in sede penale.

### 6.2. MISURE VERSO I DIPENDENTI

I dipendenti della Società devono informare tempestivamente i propri superiori gerarchici o loro referenti circa ogni circostanza che comporti, o che sembri comportare, una deviazione dalle norme di etica e di condotta indicate nel Codice Etico. Qualora, per giustificato motivo o per opportunità, sia ritenuto sconsigliabile riferire direttamente al proprio superiore gerarchico o al proprio referente, sarà cura ed onere del dipendente comunicare direttamente con l'Organismo di vigilanza. Omettere o non riferire tali circostanze costituisce una violazione del Codice Etico di cui al precedente capitolo 4 del Modello Organizzativo.

L'Organismo di vigilanza dovrà trattare le segnalazioni ricevute con la massima confidenzialità e tutte le violazioni riferite - salvo quelle anonime - saranno immediatamente oggetto di indagine. Le persone che abbiano segnalato pretese violazioni si dovranno astenere dal condurre autonomamente indagini preliminari. Le fasi istruttorie relative a tali violazioni possono infatti coinvolgere complesse questioni legali e, ponendo in essere iniziative autonome e non autorizzate, si potrebbe compromettere l'integrità e la validità dell'indagine svolta a livello istituzionale.

I dipendenti sono tenuti a cooperare e fornire le informazioni in loro possesso riguardanti tali violazioni durante le fasi istruttorie, indipendentemente dal fatto che le stesse siano considerate rilevanti. La mancata cooperazione o la cooperazione solo parziale con le attività di istruttoria possono portare a severi provvedimenti disciplinari, incluso il licenziamento.

Fermo restando quanto disposto dalle norme disciplinari del Contratto Collettivo Nazionale di Lavoro per gli addetti all'industria metalmeccanica privata e all'installazione degli impianti nonché l'inosservanza da parte del personale dipendente dei doveri e dei divieti previsti e regolati dal Codice Etico e dal Modello Organizzativo può comportare i seguenti provvedimenti, che saranno adottati in conformità con le procedure previste dall'articolo 8 della Sezione Quarta, del Titolo VII del CCNL ed in relazione all'entità dell'infrazione e alle circostanze che l'accompagneranno:

1. richiamo verbale;
2. ammonizione scritta;
3. multa in misura non eccedente l'importo di 3 ore della retribuzione oraria calcolata sul minimo tabellare;

4. sospensione dall'attività e dalla retribuzione per un massimo di 3 giorni;
5. licenziamento per mancanze con o senza preavviso.

In caso di condotte sanzionabili con il licenziamento per mancanze senza preavviso, la Società potrà disporre la sospensione cautelare non disciplinare del lavoratore/lavoratrice con effetto immediato, per un periodo massimo di 6 giorni. Ove il licenziamento venga applicato, esso avrà effetto dal momento della disposta sospensione.

A titolo indicativo:

- (A) il provvedimento del richiamo verbale e dell'ammonizione scritta di cui ai punti 1 e 2 si applicano con riferimento alle mancanze di minor rilievo tra quelle contemplate al successivo punto (B);
- (B) il provvedimento della multa di cui al punto 3 si applica nei confronti del dipendente che:
  - commetta con colpa e/o negligenza e/o imperizia una violazione non grave dei doveri e/o divieti regolati dagli artt. 4.2.1, 4.2.2, 4.2.3, 4.2.4, 4.2.5, 4.2.6, 4.2.7, 4.2.8, 4.2.9, e 4.2.10 del Codice Etico;
  - ogni volta che sia avviata una procedura formale per affrontare uno dei casi previsti dagli artt. 4.2.1.2 e 4.2.5 del Codice Etico, violi il dovere di rispettare la massima riservatezza o si rifiuti di cooperare;
  - compia atti di ritorsione nei confronti di un collega che abbia lamentato una discriminazione o una lesione dei propri diritti ai sensi degli artt. 4.2.1.2 e 4.2.5 del Codice Etico;
- (C) il provvedimento della sospensione dall'attività lavorativa e dalla retribuzione e dal servizio di cui al punto 4 si applica nei confronti del dipendente che:
  - commetta recidiva nell'anno solare in una delle violazioni sanzionate con la multa;
  - sia responsabile di atti di discriminazione indiretta;
- (D) salva ogni altra azione legale, il provvedimento di cui al punto 5 (licenziamento disciplinare con o senza preavviso) si applica per le seguenti mancanze:
  - violazione dolosa dell'art. 4.2.4.1 e 4.2.4.3;
  - abuso di informazioni riservate o confidenziali;
  - falsificazione di documenti, quali scritture contabili, documenti relativi alla Società o documenti relativi a spese di rappresentanza e trasferte;
  - violazione delle politiche di protezione e commerciali della Società, violazione del segreto industriale;
  - grave violazione anche di uno solo degli artt. 4.2.1.1, 4.2.1.2, 4.2.2.2, 4.2.2.5, 4.2.2.6, 4.2.6.1, 4.2.6.2, 4.2.6.3, 4.2.8, 4.2.9, 4.2.10 e del Codice Etico;
  - grave omessa divulgazione di informazioni importanti o intenzionale comunicazione di informazioni ingannevoli;
  - atti gravi di discriminazione diretta ed indiretta;
  - intenzionata e infondata simulazione di uno dei casi previsti dagli artt. 4.2.1.2 e 4.2.5 del Codice Etico;
  - grave violazione dell'art. 4.2.4.2 del Codice Etico o, comunque, svolgimento, in concorrenza con l'attività della Società, di altre attività, anche non remunerate, per conto proprio o di terzi, durante o al di fuori del servizio.

È a carico del Responsabile dell'Area aziendale HR il compito di organizzare e gestire il procedimento di irrogazione delle sanzioni di cui al presente Modello Organizzativo. Il Responsabile dell'Area aziendale HR riferisce all'Organismo di vigilanza riguardo l'applicazione delle sanzioni disciplinari emesse:

- il tipo e l'entità di ciascuna sanzione prevista saranno applicate, nei singoli casi, tenendo conto dei seguenti elementi;
- intenzionalità del comportamento illecito o non corretto;
- grado di negligenza, imprudenza o imperizia con riguardo alla prevedibilità dell'evento;
- condotta complessiva del dipendente (es.: eventuali precedenti), oppure l'esistenza di circostanze attenuanti (come pure anche aggravanti), tenendo in debito conto la professionalità e il suo passato lavorativo;
- il ruolo ed i compiti assegnati al dipendente;

- livello di responsabilità/posizione gerarchica, funzionale e/o tecnica;
- eventuale ipotesi di condivisione di responsabilità con altri collaboratori che abbiano concorso al comportamento manchevole.

L'applicazione delle sanzioni sarà improntata ai principi di tempestività, immediatezza ed equità.

### **6.3. MISURE VERSO I DIRIGENTI**

Il mancato rispetto delle disposizioni e regole del presente Modello Organizzativo da parte di Dirigenti di *Computer Sciences Italia srl*, tiene conto della particolare natura fiduciaria di tale rapporto di lavoro.

Nei confronti dei Dirigenti, i quali abbiano posto in essere violazioni alle Procedure, Policies, regole e/o disposizioni comunque dedotti dal presente Modello Organizzativo, la Società adotterà (nei confronti del soggetto interessato) quanto previsto dalla legge, dal codice civile e dal CCNL applicabile; nonché, le eventuali ulteriori normative speciali applicabili.

In particolare, nel caso in cui la violazione del Modello Organizzativo dovesse portare il venir meno del rapporto fiduciario con la Società, la sanzione è individuata nel licenziamento per mancanze.

### **6.4. MISURE VERSO I MEMBRI DEL CONSIGLIO DI AMMINISTRAZIONE**

L'Organismo di vigilanza deve comunicare al Collegio Sindacale e a tutti gli altri membri del Consiglio di Amministrazione della Società, comportamenti non conformi al Modello Organizzativo, posti in essere da membri del Consiglio di Amministrazione.

Il Consiglio di Amministrazione e il Collegio Sindacale procederanno ad effettuare gli accertamenti opportuni e ad assumere i provvedimenti del caso nell'ambito delle rispettive attribuzioni, ivi compresa l'eventuale convocazione dell'assemblea dei soci per la proposta di revoca dalla carica. Le relative comunicazioni saranno indirizzate direttamente a tutti i membri del Consiglio di Amministrazione e del Collegio Sindacale.

L'Organismo di vigilanza deve essere tenuto debitamente aggiornato riguardo ai provvedimenti adottati.

### **6.5. MISURE VERSO IL COLLEGIO SINDACALE**

L'Organismo di vigilanza deve comunicare a tutti gli altri membri del Collegio Sindacale e a tutti i membri del Consiglio di Amministrazione, comportamenti non conformi al Modello Organizzativo, posti in essere da membri del Collegio Sindacale.

Il Consiglio di Amministrazione e il Collegio Sindacale procederanno ad effettuare gli accertamenti opportuni e ad assumere i provvedimenti del caso nell'ambito delle rispettive attribuzioni, ivi compresa l'eventuale convocazione dell'assemblea dei soci per la proposta di revoca dalla carica. Le relative comunicazioni saranno indirizzate direttamente a tutti i membri del Consiglio di Amministrazione e del Collegio Sindacale.

L'Organismo di vigilanza deve essere tenuto debitamente aggiornato riguardo ai provvedimenti adottati.

### **6.6. MISURE VERSO TERZI**

Nell'ambito di rapporti di partnership e/o di collaborazione esistenti con: Consulenti, Collaboratori, o comunque terze parti; è preciso dovere di *Computer Sciences Italia srl* prevedere opportune misure che prevedano efficaci meccanismi deterrenti, nonché, nei casi più gravi, anche risolutivi.

Infatti, i comportamenti delle terze parti, anche di natura omissiva, che comportino violazioni e condotte in contrasto con le disposizioni e principi del presente Modello Organizzativo, potranno



determinare la risoluzione del rapporto contrattuale, nonché la richiesta di risarcimento nel caso derivino danni alla Società.

## 7. FORMAZIONE, COMUNICAZIONE E DIFFUSIONE

E' preciso impegno di *Computer Sciences Italia srl* dare ampia divulgazione, all'interno ed all'esterno della Società dei principi contenuti nel presente Modello Organizzativo.

A tal fine, *Computer Sciences Italia srl* pone in essere opportune iniziative atte a promuovere e a diffondere la conoscenza del presente Modello Organizzativo, avendo cura di operare una necessaria diversificazione di approfondimento a seconda del ruolo, responsabilità e compito in Società.

Il presente Modello Organizzativo è comunicato formalmente secondo le modalità di seguito descritte.

### 7.1. COMUNICAZIONE VERSO L'INTERNO

#### 7.1.1. Comunicazione e formazione in generale

Al fine di assicurare la più completa ed ampia diffusione dei principi e delle regole previste dal presente Modello Organizzativo, questo è reso disponibile a tutti i dipendenti di *Computer Sciences Italia srl* sul repository denominato SGPA, per mezzo della rete intranet aziendale, nonché tramite il portale ed il sito internet della Società.

I dipendenti sono informati della redazione e dei successivi aggiornamenti del Modello Organizzativo.

Per tutti i dipendenti sono realizzate opportune attività di informazione (quali ad es. invio di email di aggiornamento, di comunicazione, etc..) oppure, iniziative di formazione in collaborazione con l'Area aziendale HR.

La comunicazione riguarda a titolo esemplificativo:

- il Codice Etico;
- i diversi poteri autorizzativi;
- le linee di dipendenza gerarchica;
- le Procedure;
- i flussi di informazione e tutto quanto contribuisca a dare trasparenza nell'operare quotidiano.

Per i dipendenti, in funzione del loro specifico ruolo nell'ambito delle attività oggetto di mappatura ai fini del Modello Organizzativo sono organizzate sessioni formative erogate anche per mezzo di soluzioni informatiche disponibili (es.: workshop via intranet, teleconferenze, etc.) e supportate da materiale formativo appositamente realizzato.

#### 7.1.2. Comunicazione e formazione in materia di sicurezza e salute dei lavoratori

La Società ha predisposto un adeguato e specifico sistema di comunicazione e formazione del personale di *Computer Sciences Italia srl* al fine di prevenire la commissione dei reati in materia di sicurezza e salute dei lavoratori.

Infatti la circolazione delle informazioni all'interno della Società assume un valore rilevante per favorire il coinvolgimento di tutti i soggetti interessati e consentire consapevolezza ed impegno adeguati a tutti i livelli.

Il coinvolgimento è realizzato attraverso riunioni periodiche che tengano conto delle richieste fissate dalla legislazione vigente utilizzando anche le riunioni previste per la gestione aziendale.

Lo svolgimento dei compiti che possono influenzare la salute e sicurezza sul lavoro richiede una adeguata competenza, che occorre verificare ed alimentare.

A tal fine sono organizzati corsi di formazione finalizzati ad assicurare che tutto il personale, ad ogni livello, sia consapevole della importanza della conformità delle proprie azioni rispetto al

Modello Organizzativo e delle possibili conseguenze dovute a comportamenti che si discostino dalle regole dettate dal Modello Organizzativo con particolare riferimento alla prevenzione dei reati in tema di salute e sicurezza dei lavoratori.

I corsi si svolgono in via telematica mediante quesiti scritti e saranno organizzati distinguendo il personale di *Computer Sciences Italia srl* con riferimento al loro posto di lavoro e alle loro mansioni.

Il corso di formazione si tiene:

- in occasione dell'assunzione;
- periodicamente secondo i fabbisogni rilevanti della Società.

### **7.1.3. Comunicazione e formazione**

Oltre a quanto sopra previsto, i principi, le regole e le disposizioni del presente Modello Organizzativo, anche con riferimento alla tutela della salute e sicurezza dei lavoratori, sono comunicati in maniera più specifica e mirata ai seguenti soggetti aziendali:

- membri del CdA;
- Responsabili delle Aree aziendali e Responsabili delle Funzioni aziendali;
- Dirigenti;
- tutto il personale che, in ragione dell'attività, ruolo o mansione ricoperta in Società, risulti particolarmente coinvolto in Processi a rischio di reati previsti dal Decreto.

Il piano delle iniziative di comunicazione e formazione anche relativo alla prevenzione dei reati in materia di salute e sicurezza dei lavoratori è definito dall'Organismo di vigilanza, coadiuvato e in coordinamento con l'Area aziendale HR.

## **7.2. DIFFUSIONE VERSO L'ESTERNO**

Nel rispetto dei principi fondamentali di *Computer Sciences Italia srl*, legati alla trasparenza, correttezza e integrità, l'adozione del Modello Organizzativo è comunicata e diffusa anche ai soggetti esterni all'azienda, quali clienti, fornitori, partners e terzi in genere.

I documenti descrittivi del Modello Organizzativo sono inoltre messi a disposizione sul sito internet di *Computer Sciences Italia srl*.

L'avvenuta comunicazione e l'impegno formale da parte dei suddetti soggetti esterni verso *Computer Sciences Italia srl*, al rispetto dei principi del Codice Etico di *Computer Sciences Italia srl* e del presente Modello Organizzativo, sono documentati attraverso la predisposizione di specifiche dichiarazioni o clausole contrattuali debitamente sottoposte ed accettate dalla controparte.

In merito agli adempimenti circa la comunicazione e diffusione all'esterno, si richiamano in particolare le seguenti responsabilità:

- ciascun Responsabile dell'Area aziendale e Responsabile della Funzione aziendale è responsabile di mantenere la corretta comunicazione sia al proprio interno, sia l'esterno dell'azienda, per ciò che concerne l'adozione e attuazione del Modello Organizzativo;
- l'Organismo di vigilanza effettua un'attività di supporto alle altre Funzioni aziendali, quando si debbano dare informazioni all'esterno di *Computer Sciences Italia srl* relative al Modello Organizzativo.

**FINE DOCUMENTO**

