

Estratto del Modello di organizzazione e controllo

RESPONSABILITA' AMMINISTRATIVA DELLE IMPRESE

**ai sensi del D.Lgs. 231/01
T-Systems Italia S.p.A.**

**Approvato dal Consiglio di Amministrazione di T-Systems Italia S.p.A.
in data 19 marzo 2008 e aggiornato in data 3 novembre 2008**

Indice

1. Premesse	4
2. Obiettivo	5
3. Descrizione di T-Systems	7
a) <i>Aspetti generali</i>	7
b) <i>Assetto societario</i>	7
c) <i>Organigramma</i>	7
d) <i>Vicende pregresse</i>	7
e) <i>Ambito di applicazione del Modello</i>	7
4. Mappatura delle misure attualmente in essere a contenimento del rischio di reati	9
a) <i>Reati nei confronti della pubblica amministrazione</i>	10
b) <i>Reati societari</i>	15
c) <i>Reati con finalità di terrorismo</i>	18
d) <i>Reati contro la persona</i>	19
e) <i>Reati di abuso di mercato</i>	20
f) <i>Reati transnazionali ex lege 146/06</i>	21
g) <i>Omicidio colposo e lesioni colpose gravi</i>	23
j) <i>Reati di corruzione tra privati</i>	26
5. Modello organizzativo	27
a) <i>Codici di comportamento</i>	27
b) <i>Misure a contenimento del rischio di reati</i>	27
b.1) <i>Reati nei confronti della pubblica amministrazione</i>	28
b.2) <i>Reati societari</i>	29
b.3) <i>Reati con finalità di terrorismo</i>	29
b.4) <i>Reati contro la persona</i>	30
b.5) <i>Reati di abuso di mercato</i>	30
b.6) <i>Reati transnazionali ex lege 146/06</i>	30
b.7) <i>Reati in materia di sicurezza sul lavoro</i>	31
b.10) <i>Appendice su Advisory Board</i>	32
c) <i>Organismo di Vigilanza</i>	33
c.1) <i>Indipendenza</i>	33
c.2) <i>Risorse</i>	33
c.3) <i>Composizione - Durata</i>	33
c.4) <i>Competenze</i>	34
c.5) <i>Attività di reporting dell'OdV</i>	35
c.6) <i>Reporting verso l'OdV</i>	35
c.7) <i>Raccolta e conservazione delle informazioni</i>	36
d) <i>Sistema sanzionatorio</i>	37
d.1) <i>Per i dipendenti</i>	37
d.2) <i>Per gli Amministratori</i>	38
d.3) <i>Per i Sindaci</i>	38
d.4) <i>Per l'Organismo di Vigilanza</i>	38
d.5) <i>Per i partner, consulenti e fornitori</i>	38
e) <i>Piano di formazione</i>	39
f) <i>Piano di informazione</i>	41

Allegati:

- 1. Reati rilevanti ai sensi del D.Lgs. 231/01**
- 2. Composizione del consiglio di Amministrazione**
- 3. Organigramma Funzionale**
- 4. Composizione Advisory Board**
- 5. Sistema di Gestione della Salute e della Sicurezza sul Lavoro**

1. Premesse

T-Systems Italia S.p.A. (di seguito “T-Systems”) con riferimento alla disciplina della responsabilità amministrativa delle società per taluni reati, introdotta con il D.Lgs. 231/01 ha inteso procedere all’introduzione di un proprio Modello di Organizzazione e Controllo (di seguito il “Modello”). Tale introduzione è inserita in un più ampio processo di verifica dei modelli di indirizzo e controllo previsti dalla Corporate Governance.

In conseguenza di ciò è stato creato un organismo in ogni paese in cui è presente T-Systems denominato Compliance Committee che ha come obiettivo primario quello di verificare il rispetto e l’osservanza delle regole e dei principi interni ed esterni alla società. Il Compliance Committee coordinerà la propria attività con l’Organismo di Vigilanza.

Il presente Modello è stato adottato dal Consiglio di Amministrazione di T-Systems con delibera del 19 marzo 2008 ed aggiornato con delibera del Consiglio di Amministrazione del 3 novembre 2008.

Essendo T-Systems un membro di Confindustria, nella predisposizione del presente Modello si è ispirata alle linee guida da quest’ultima approvate il 7 marzo 2002 e di seguito aggiornate. In particolare l’attuale aggiornamento di modello organizzativo tiene conto delle Linee Guida di Confindustria nella versione del 31 marzo 2008.

Resta inteso che la scelta di non adeguare il Modello ad alcune indicazioni di cui alle linee guida di Confindustria non inficia la validità dello stesso. Il singolo Modello, al contrario, dovendo essere redatto con riferimento alla realtà concreta della società, ben può discostarsi dalle sopra richiamate linee guida, che per loro natura, hanno carattere generale.

Le regole di comportamento contenute nel presente Modello, inoltre, sono coerenti con quelle del Codice Etico adottato da T-Systems il 20 novembre 2003, pur avendo il presente Modello finalità specifiche in ottemperanza al D.Lgs. 231/01.

Il Modello di T-Systems è composto da:

- a) il presente documento;
- b) i codici di comportamento e le procedure organizzative già in vigore all’interno di T-Systems e che siano attinenti ai fini del controllo di comportamenti, fatti o atti rilevanti ex D.Lgs. 231/01 tra i quali:
 - Statuto Sociale;
 - sistema di deleghe interne (poteri delegati dal Consiglio di Amministrazione e Procure o Deleghe generali e particolari);
 - Codice Etico;
 - Code of Conduct di Deutsche Telekom;
 - le procedure aziendali e del Gruppo T-Systems, la documentazione e le disposizioni inerenti la struttura gerarchico – funzionale aziendale ed organizzativa del Gruppo T-Systems ed il sistema del controllo della gestione;
 - le norme inerenti il sistema amministrativo, contabile, finanziario, informatico e di reporting di T-Systems;
 - principi di Corporate Governance (Compliance Committee).

I codici di comportamento e le procedure sopra elencate, pur non essendo stati emanati esplicitamente ai sensi del D.Lgs. 231/01 hanno tra i loro obiettivi il controllo della regolarità, diligenza e legalità del comportamento di coloro che rappresentano o sono dipendenti di T-Systems e, pertanto, contribuiscono ad assicurare la prevenzione dei reati di cui al D.Lgs. 231/01.

I principi, le regole e le procedure di cui agli strumenti sopra elencati, non vengono riportati dettagliatamente nel presente Modello, ma fanno parte del più ampio sistema di organizzazione e controllo che lo stesso intende integrare.

2. Obiettivo

Obiettivo del presente documento è la definizione dei modelli di organizzazione, di gestione e controllo prescritti dal D.Lgs. 231/01. Lo scopo di tali modelli è quello di prevenire i reati per i quali la legge in questione prescrive la responsabilità amministrativa dell'impresa.

I reati, espressamente indicati dalla legge, sono riconducibili ad otto categorie:

1. reati contro la pubblica amministrazione;
2. reati societari;
3. reati con finalità di terrorismo e di eversione dell'ordine democratico;
4. reati contro la persona;
5. reati di manipolazione del mercato;
6. reati transnazionali di cui alla legge 146/06;
7. reati di omicidio colposo, lesioni gravi o gravissime commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro;
8. reati di ricettazione, riciclaggio e impiego di denaro, beni o altre utilità di provenienza illecita;
9. reati informatici.

In considerazione del fatto che le categorie dei reati presupposto saranno a breve integrati con quella relativa ai reati di corruzione tra privati, il Modello, nella parte relativa all'analisi dei rischi si estende anche a questa categoria di reato nonostante non sia ancora oggetto di una normativa approvata.

Per il dettaglio dei reati si veda l'Allegato 1.

La responsabilità dell'impresa è prevista nei casi in cui i reati siano posti in essere nell'interesse o a vantaggio della stessa da soggetti in posizione apicale o da soggetti posti sotto la direzione o la vigilanza dei primi.

Nel primo caso, l'impresa non risponde se prova che:

- a) l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi;
- b) il compito di vigilare sul funzionamento e l'osservanza dei modelli e di curare il loro aggiornamento è stato affidato a un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo;
- c) le persone hanno commesso il reato eludendo fraudolentemente i modelli di

T-Systems Italia S.p.A.

Modello Organizzativo di Controllo

3 novembre 2008

Documento Interno

organizzazione e di gestione;

d) non vi è stata omessa o insufficiente vigilanza da parte dell'organismo di cui alla lettera b).

Nel secondo caso, l'impresa è responsabile se il reato è stato reso possibile dall'inosservanza degli obblighi di direzione o di sorveglianza. In ogni caso è esclusa l'inosservanza di tali obblighi, se si è adottato un modello di organizzazione, gestione e controllo volto a prevenire il reato.

In ragione di ciò, il perimetro di intervento del Modello è rappresentato dall'azienda T-Systems. Per le considerazioni in merito all'estensione dei modelli ad altri soggetti, sui quali la società esercita un controllo o dalle cui azioni potrebbe subire conseguenze, si rimanda al capitolo 2 lett. e).

Per la definizione del Modello si è proceduto conformemente a quanto disposto dalla legge e sulla base delle indicazioni fornite dalle associazioni di categoria, in particolare di Confindustria.

Si è effettuata, quindi:

- la mappatura delle aree a rischio;
- la mappatura delle principali modalità di attuazione degli illeciti nelle aree a rischio;
- la mappatura dei sistemi di controllo preventivi in essere;
- l'individuazione degli adeguamenti necessari al sistema di controllo;
- la definizione del Modello, attraverso la descrizione di:
 - le procedure;
 - il codice etico;
 - l'Organismo di Vigilanza;
 - il sistema sanzionatorio;
 - il piano di formazione e informazione per i dipendenti.

3. Descrizione di T-Systems

a) Aspetti generali

T-Systems Italia S.p.A. è una società del Gruppo Deutsche Telekom che fornisce servizi ICT a clienti business, sia pubblici che privati.

Ha circa 700 dipendenti nelle sedi di Assago-Milanofiori, Mirandola (MO), Napoli, Roma e Vicenza.

b) Assetto societario

E' una società a socio unico. Il 100% delle azioni è detenuta da T-Systems Enterprise Services GmbH, a sua volta posseduta al 100% da Deutsche Telekom.

In Allegato 2 la composizione del Consiglio di Amministrazione.

T-Systems non detiene quote maggioritarie in altre società.

c) Organigramma

L'organigramma funzionale, è riportato in Allegato 3.

Nel marzo 2007 è stato poi istituito l'Advisory Board con funzioni meramente consultive su piani strategici, di competenze ed evoluzione tecnologica. Il board è composto da personalità di alto profilo professionale così come descritto in Allegato 4.

Ogni volta che si riunisce viene redatto verbale.

d) Vicende pregresse

Non risultano nella storia dell'azienda vicende riconducibili a procedimenti penali legati alla commissione di reati, di cui al D.Lgs. 231/01.

e) Ambito di applicazione del Modello

Il Modello si applica all'azienda T-Systems. Si fa, tuttavia, presente che:

- a breve tali modelli verranno estesi anche alla società T-Systems Spring Italia srl che, pur non essendo partecipata da T-Systems ma da T-Systems Enterprise Services GmbH, è soggetta al controllo di T-Systems in quanto rappresentanti di quest'ultima siedono nel Consiglio di Amministrazione di T-Systems Spring Italia srl;
- per quanto riguarda il Fondo Pensioni (Fondo aziendale di previdenza a capitalizzazione per il personale dipendenti di T-Systems), esso è stato costituito come associazione non riconosciuta ai sensi dell'art. 36 del codice civile. Non è,

- quindi, un organismo interno all'azienda ma un ente esterno che, pur essendo privo di personalità giuridica, può rispondere direttamente ai sensi del D.Lgs. 231/01. Lo Statuto prevede la nomina nel Consiglio di Amministrazione del Fondo di un numero pari di rappresentanti dei dipendenti e dell'azienda. In ragione di ciò, non può escludersi che T-Systems sia chiamata a rispondere per eventuali illeciti posti in essere dal Fondo a suo vantaggio o nel suo interesse. Tuttavia, per la peculiare natura dell'attività del Fondo, ad esso non può essere esteso/imposto il modello di T-Systems. Quest'ultima sottoporrà al Consiglio di Amministrazione del Fondo la proposta di adottare propri modelli organizzativi;
- per quanto riguarda l'attività che la capogruppo dovesse svolgere in Italia e comunque a vantaggio o nell'interesse di T-Systems, quest'ultima la informerà dell'adozione del Modello e la solleciterà al rispetto dello stesso nello svolgimento dell'attività suddetta.

4. Mappatura delle misure attualmente in essere a contenimento del rischio di reati

La tabella che segue riporta, per ogni categoria di reato, le procedure adottate da T-Systems (documentazione/procedure evidenziate nella tabella mediante sottolineatura) che, pur introdotte per altre finalità (organizzative, produttive o per adempiere a vincoli normativi o a standard internazionali), rappresentano una misura adeguata a contenere il rischio dei reati analizzati.

L'identificazione delle misure e la relativa adeguatezza sono valutate tenendo conto delle indicazioni fornite dalle associazioni di categoria, in particolare Confindustria e Assogestioni (per i reati di abuso di mercato).

La mappa riporta per ogni singola categoria di reato, le misure in essere riconducendole, ove possibile, alla categorizzazione utilizzata dalle associazioni di categoria. Queste ultime hanno, infatti, provveduto nelle rispettive Linee Guida a dare indicazione di alcune aree di intervento a contenimento dei vari rischi di reato (in corsivo).

a) Reati nei confronti della pubblica amministrazione

REATI DI CORRUZIONE			
Corruzione per un atto d'ufficio	Corruzione per un atto contrario ai doveri d'ufficio	Corruzione in atti giudiziari	Istigazione alla corruzione
<i>Esplicita previsione tra i principi etici (Confindustria)</i>			
<u>Codice deontologico di Gruppo:</u> Pag. 14 Conflitto di interessi Pag. 15 Donazioni			
<u>Codice Etico Italia:</u> 2.2.3 Doni e favori 3.1 Clienti 3.9 Pubbliche amministrazioni e Istituzioni			
<u>Fraud Management Process:</u> Obblighi di segnalazione alla casa madre di eventuali frodi (attraverso l'Auditing)			
<i>Sistema di deleghe (Confindustria)</i>			
I poteri di firma e le deleghe sono assegnati rispettando la struttura organizzativa e ricorrendo nelle aree più sensibili alla doppia firma. Nei casi in cui è prevista la doppia firma, talvolta è richiesto che una delle due provenga da una funzione determinata (firma obbligatoria). Sono esplicitamente indicate delle soglie di approvazione delle spese e dei livelli di autorizzazione per la stipula dei contratti			
<i>Misure nei rapporti con i terzi collaboratori (Confindustria)</i>			
<u>Misure Sox/Purchasing/ 24000260-24000261:</u> Le misure sono volte a garantire la corretta selezione dei collaboratori/prestatori di servizi. Qui rilevano ai fini della selezione di terzi collaboratori che operano nei rapporti con la PA in modo da ridurre la probabilità che si producano situazioni a rischio corruzione.			
<u>Global Procurement Practices della Corporate:</u> <u>Purchasing Policy di T-Systems Italia spa</u> (di cui in particolare il <u>Suppliers Management Process (SUM)</u> <u>Procedura SAP</u> <u>Utilizzo della PO Checklist</u> Le misure sono volte a garantire una disciplina certa e trasparente per l'acquisto di beni e servizi. Qui rilevano per garantire trasparenza nella selezione di consulenti (commerciali e non) e fornitori Procedure per l'acquisizione di beni e servizi mediante aste on line (procedure per eAuction)			
<i>Controllo sui flussi finanziari aziendali (Confindustria)</i>			
<u>Procedura SAP</u> per gestione acquisti e pagamenti Le spese non previste dal budget sono espressamente autorizzate. L'autorizzazione prevede il controllo incrociato del Responsabile dell'area del richiedente e della funzione di Controlling. Il Responsabile dell'ordine di acquisto approva il pagamento in modo che sia garantita la verifica dell'esistenza non meramente contabile delle prestazioni effettuate da terzi			
<i>Controllo dei sistemi informativi</i>			
<u>Misure Sox/Information Technology/24000288-24000289-24000290</u> Le misure sono volte a garantire la correttezza delle transazioni batch e on line e la produzione dei relativi report Qui rilevano per garantire il monitoraggio delle tecnologie utilizzate per i pagamenti			
Politica di sicurezza delle Informazioni: <u>Certificazione 27001, SAS 70</u> Qui rileva per garantire il monitoraggio dell'uso delle tecnologie a cui si ricorre per i pagamenti			
<u>Misure Sox/Information Technology/24000291-24000292-24000293-2400094-2400095</u> Si tratta di misure volte a garantire l'efficienza e l'adeguatezza del sistema informativo di			

<p>produzione e di gestione del business. Qui rilevano ai fini di ridurre la probabilità che si producano situazioni a rischio corruzione volte a coprire inefficienze dei servizi o inadempimenti contrattuali nei confronti della pa</p>
<p><i>Conservazione e controllo della documentazione aziendale (Confindustria)</i></p>
<p><u>Misure Sox/Sales/24000118-119-121-122-127-128-132-133-607</u> Le misure sono volte alla conservazione e aggiornamento delle informazioni relative alle vendite Qui rilevano, limitatamente ai rapporti con la PA, ai fini di consentire il controllo sulla documentazione relativa allo svolgimento dell'attività di vendita</p>
<p><u>Misure Sox/Sales/24000124-125-129-130</u> Le misure sono volte al controllo dell'attività di vendita. Qui rilevano, limitatamente ai rapporti con la PA, ai fini di consentire il controllo sul rispetto della disciplina interna relativa allo svolgimento dell'attività di vendita.</p>
<p><u>DPS/6.2 Contromisure per l'integrità dei dati</u> Le misure sono volte a ridurre il rischio di perdita o modifica dei dati personali. Qui rilevano con riferimento all'esigenza di conservare la documentazione aziendale anche su supporto informatico</p>
<p><u>DPS/7 Misure di Sicurezza Logiche, Fisiche e Organizzative</u> Le misure sono adottate in adempimento al disciplinare tecnico ex d.lgs. 196/03. Qui rilevano in quanto volte a garantire l'integrità e la disponibilità dei dati</p>
<p><u>DPS/7.3.9 Controllo e procedure di controllo accessi agli archivi cartacei</u> Le misure disciplinano l'accesso e la disponibilità della documentazione su supporto cartaceo. Qui rilevano per gli aspetti relativi alla conservazione della documentazione (armadi chiusi, contenitori etc.)</p>
<p>Politica di sicurezza delle Informazioni: <u>Certificazione 27001, SAS 70</u> Qui rileva per garantire l'integrità e la disponibilità dei dati</p>
<p><u>Piano di Business Continuity</u> Qui rileva per garantire l'integrità e la disponibilità dei dati</p>
<p><u>Piano di Disaster Recovery</u> Qui rileva per garantire l'integrità e la disponibilità dei dati</p>
<p>Procedura che prevede la conservazione della documentazione su supporto cartaceo e su supporto informatico (<u>Livelink</u>) utilizzato da Ufficio Legale, Ufficio Acquisti e segreteria per protocollo della posta</p>
<p><i>Sistema premiante equilibrato che non induca a comportamenti illeciti pur di raggiungere gli obiettivi (Confindustria)</i></p>
<p>La remunerazione della forza vendite è costituita da una quota fissa (circa il 70%) e da una variabile (circa il 30%). La quota variabile è determinata da parametri aziendali complessivi, dall'ordinato, dal fatturato e dall'acquisizione di nuovi clienti.</p>
<p><i>Procedure per omaggi e sponsorizzazioni (Confindustria)</i></p>
<p>La scelta degli omaggi è attribuita al Marketing&Communications La sponsorizzazione di iniziative è definita dal M&C e approvata dall'AD. I contributi a onlus e iniziative benefiche sono stati vagliati dal M&C e da F&C. Eventi quali viaggi, partecipazione a convegni etc. rivolti alla clientela, anche pubblica, sono decisi dal M&C</p>
<p><i>Procedure di assunzione del personale</i></p>
<p>La selezione dei candidati viene effettuata dalla Direzione del Personale che provvede generalmente su indicazione dell'area coinvolta. La procedura prevede la richiesta del certificato penale.</p>
<p><i>Misure volte a ridurre il rischio di pratiche corruttive volte a coprire inadempimenti contrattuali nei confronti della pa</i></p>
<p><u>Service Management (SEM)</u> Le procedure sono stabilite per consentire una corretta gestione della fase iniziale di transizione del servizio, della fase a regime e di quella di fine servizio (con il rinnovo o l'estinzione) Qui rilevano per ridurre il rischio di inadempimenti contrattuali nei confronti della pa, grazie anche</p>

ad una puntuale individuazione di compiti e responsabilità dei soggetti coinvolti.			
<u>Linee Guida Application Management</u> Le procedure sono volte a garantire i livelli di servizio e i deliverables contenuti all'interno dei contratti stipulati con i clienti. Qui rilevano per ridurre il rischio di inadempimenti contrattuali nei confronti della pa			
<u>Sistema di qualità ISO9001</u> che copre tutta l'attività aziendale dalla progettazione alla delivery Qui rileva per ridurre il rischio di inadempimenti contrattuali nei confronti della pa			
REATI DI FRODE AI DANNI DELLO STATO			
Malversazione a danno dello Stato	Indebita percezione di erogazioni a danno dello Stato	Truffa e truffa aggravata per il perseguimento di erogazioni pubbliche	Frode informatica
<i>Esplícita previsione tra i principi etici (Confindustria)</i>			
<u>Codice Etico Italia</u> 2.2.2. Responsabilità nell'utilizzo del tempo e dei beni aziendali Qui rileva ai fini di contenere il rischio di uso improprio delle strumentazioni informatiche			
<u>Fraud Management Process</u> Obblighi di segnalazione alla casa madre di eventuali frodi (attraverso l'Auditing)			
<i>Misure nei rapporti con i terzi collaboratori</i>			
<u>Misure Sox/Purchasing/ 24000260-24000261</u> Si tratta di misure volte a garantire la corretta selezione dei collaboratori/prestatori di servizi. Qui rilevano ai fini della selezione di terzi collaboratori che operano nei rapporti con la PA in modo da ridurre la probabilità che si producano situazioni a rischio frode			
<u>Global Procurement Practices della Corporate Purchasing Policy di T-Systems Italia spa</u> (di cui in particolare il <u>Suppliers Management Process (SUM)</u> <u>Procedura SAP</u> <u>Utilizzo della PO Checklist</u> Le misure sono volte a garantire una disciplina certa e trasparente per l'acquisto di beni e servizi. Qui rilevano per garantire trasparenza nella selezione di consulenti (commerciali e non) e fornitori			
<i>Controllo sui flussi finanziari aziendali</i>			
<u>Procedura SAP</u> . La verifica è affidata al Finance			
<i>Separazione funzionale tra chi gestisce le attività realizzative e chi presenta la documentazione alla PA (Confindustria)</i>			
La procedura prevede che la documentazione per la richiesta di eventuali finanziamenti sia predisposta dall'Ufficio Legale in collaborazione con l'area aziendale coinvolta dalla richiesta (BPO per Academy, Direzione del Personale per finanziamenti a formazione interna etc.). La documentazione è sottoscritta dal rappresentante legale.			
<i>Specifiche attività di controllo gerarchico su documentazione da presentare (relativamente sia alla documentazione di progetto che alla documentazione attestante i requisiti tecnici, economici e professionali dell'azienda che presenta il progetto). (Confindustria)</i>			
La procedura gare prevede che: <ul style="list-style-type: none"> - il bando sia verificato dal Proposal Manager (area vendite) con l'Ufficio Legale (di seguito UL) - la valutazione della capacità economica sia verificata dall'Ufficio Legale in collaborazione con il Controlling e il Proposal Manager. - la valutazione della capacità tecnica sia verificata dalla Solution dell'area tecnica - in caso positivo, si organizza un team di lavoro composto dall'UL competente a redigere la documentazione amministrativa, Solution dell'area tecnica competente a redigere l'offerta tecnica, l'area vendite per l'offerta economica. La funzione di coordinamento e assistenza interpretativa è svolta dall'UL. - il confezionamento della documentazione della presentazione è affidata a RM all'area 			

<p>commerciale, a Milano all'UL</p> <p>- l'UL conserva la documentazione presentata su supporto cartaceo e informatico</p> <p>Nel caso si decida di partecipare attraverso un RTI, l'UL mantiene la funzione di coordinamento e assistenza, provvedendo alla raccolta della documentazione amministrativa necessaria e al collegamento con lo studio notarile.</p>
<p><i>Coerenza delle procure verso l'esterno con il sistema delle deleghe (Confindustria)</i></p>
<p>I poteri di firma e le deleghe sono assegnati rispettando la struttura organizzativa e ricorrendo nelle aree più sensibili alla doppia firma. Nei casi in cui è prevista la doppia firma, talvolta è richiesto che una delle due provenga da una funzione determinata (firma obbligatoria). Sono esplicitamente indicate delle soglie di approvazione delle spese e dei livelli di autorizzazione per la stipula dei contratti</p>
<p><i>Controllo dei sistemi informativi</i></p>
<p><u>Misure Sox/Information Technology/24000288-24000289-24000290</u> Si tratta di misure volte a garantire la correttezza delle transazioni batch e on line e la produzione dei relativi report Qui rilevano per garantire il monitoraggio delle tecnologie utilizzate nei rapporti con la PA</p>
<p><u>Misure Sox/Information Technology/24000291-24000292-24000293-2400094-2400095</u> Si tratta di misure volte a garantire l'efficienza e l'adeguatezza del sistema informativo di produzione e di gestione del business. Qui rilevano ai fini di ridurre la probabilità che si producano situazioni a rischio di frode nei confronti della PA</p>
<p><u>DPS/7.3.4 Sicurezza nella trasmissione dei dati</u> Si tratta di misure volte a proteggere le connessioni di rete Qui rilevano ai fini di garantire il monitoraggio della rete per rilevare possibili utilizzi in frode ai sistemi informatici pubblici</p>
<p><u>DPS/7.3.5 Installazione di software non autorizzato</u> Si tratta di una misura volta ad impedire l'utilizzo di software in violazione delle norme in materia di diritto d'autore Qui rileva ai fini di impedire l'uso di sw che consenta la frode informatica</p>
<p>Politica di sicurezza delle Informazioni: <u>Certificazione 27001, SAS 70</u> Qui rileva per garantire il monitoraggio dell'utilizzo delle tecnologie</p>
<p><i>Conservazione e controllo della documentazione aziendale</i></p>
<p><u>Misure Sox/Sales/24000118-119-121-122-132-133-607</u> Si tratta di misure volte alla conservazione e aggiornamento delle informazioni relative alle vendite Qui rilevano, limitatamente ai rapporti con la PA, ai fini di consentire il controllo sulla documentazione relativa allo svolgimento dell'attività di vendita</p>
<p><u>Misure Sox/Sales/24000124-125-130</u> Si tratta di misure volte al controllo dell'attività di vendita. Qui rilevano, limitatamente ai rapporti con la PA, ai fini di consentire il controllo sul rispetto della disciplina interna relativa allo svolgimento dell'attività di vendita.</p>
<p><u>Misure Sox/Sales/24000127-128-129</u> Si tratta di misure volte al controllo e alla documentazione dell'attività di vendita per gli aspetti relativi all'iva e alle tasse doganali Qui rilevano, limitatamente ai rapporti con la PA, ai fini di consentire il controllo sulla documentazione relativa agli aspetti in questione</p>
<p><u>DPS/6.2 Contromisure per l'integrità dei dati</u> Si tratta di misure volte a ridurre il rischio di perdita o modifica dei dati personali. Qui rilevano con riferimento all'esigenza di conservare la documentazione aziendale anche su supporto informatico</p>
<p><u>DPS/7 Misure di Sicurezza Logiche, Fisiche e Organizzative</u> Si tratta delle misure adottate in adempimento al disciplinare tecnico ex d.lgs. 196/03. Qui rilevano in quanto volte a garantire l'integrità e la disponibilità dei dati</p>
<p><u>DPS/7.3.9 Controllo e procedure di controllo accessi agli archivi cartacei</u></p>

<p>Si tratta di misure che disciplinano l'accesso e la disponibilità della documentazione su supporto cartaceo.</p> <p>Qui rilevano per gli aspetti relativi alla conservazione della documentazione (armadi chiusi, contenitori etc.)</p>
<p>Politica di sicurezza delle Informazioni: <u>Certificazione 27001, SAS 70</u></p> <p>Qui rileva per garantire l'integrità e la disponibilità dei dati</p>
<p><u>Piano di Business Continuity</u></p> <p>Qui rileva per garantire l'integrità e la disponibilità dei dati</p>
<p><u>Piano di Disaster Recovery</u></p> <p>Qui rileva per garantire l'integrità e la disponibilità dei dati</p>
<p>Procedura che prevede la conservazione della documentazione su supporto cartaceo e su supporto informatico (<u>Livelink</u>) utilizzato da Ufficio Legale, Ufficio Acquisti e segreteria per protocollo della posta</p>
<p><i>Sistema premiante equilibrato che non induca a comportamenti illeciti pur di raggiungere gli obiettivi (Confindustria)</i></p>
<p>La remunerazione della forza vendite è costituita da una quota fissa (circa il 70%) e da una variabile (circa il 30%). La quota variabile è determinata da parametri aziendali complessivi, l'ordinato, il fatturato e l'acquisizione di nuovi clienti.</p>
<p><i>Procedure per omaggi e sponsorizzazioni (Confindustria)</i></p>
<p>La scelta degli omaggi è attribuita al Marketing&Communications</p> <p>La sponsorizzazione di iniziative è definita dal M&C e approvata dall'AD. I contributi a onlus e iniziative benefiche sono stati vagliati dal M&C e da F&C.</p> <p>Eventi quali viaggi, partecipazione a convegni etc. rivolti alla clientela, anche pubblica, sono decisi dal M&C</p>

b) Reati societari

FALSE COMUNICAZIONI SOCIALI		
False comunicazioni sociali in danno della società, dei soci o dei creditori.	Falso in prospetto	Falsità nelle relazioni o nelle comunicazioni delle società di revisione.
Illecita influenza sull'assemblea	Aggiotaggio	Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza
<i>Esplicita previsione tra i principi etici (Confindustria)</i>		
<p><u>Codice deontologico di Gruppo</u> Pag. 14 Conflitto di interessi Pag. 15 Collaborazione con i terzi Qui rileva limitatamente ai rischi di aggioaggio</p>		
<p><u>Codice Etico Italia</u> 2.3 Riservatezza e privacy 3.6 Rapporti con gli organi di informazione 3.10 Uso di informazioni interne Qui rileva limitatamente ai rischi di aggioaggio</p>		
<i>Procedura rivolta alle funzioni aziendali con cui si stabiliscono le modalità per garantire la produzione delle informazioni di bilancio e la corretta trasmissione delle stesse agli organi deputati (Confindustria)</i>		
<p><u>Misure Sox/ Financial statements/all</u> Si tratta di procedure volte a garantire la corretta produzione dei dati relativi alla situazione finanziaria</p>		
<p><u>Misure Sox/Treasury/all</u> Si tratta di procedure volte a garantire che tutti gli items siano calcolati correttamente, che le transazioni finanziarie registrate riflettano circostanze e condizioni economiche reali in accordo con le regole di contabilità e che le riserve siano disposte in modo adeguato</p>		
<p><u>Misure Sox/Noncurrent assets/all</u> Si tratta di misure volte a documentare e controllare nuovi investimenti, nuovi prestiti, cambi azionari, nuove modifiche normative, e a monitorare perdite e rischi finanziari</p>		
<p><u>Misure Sox/Sales/all</u> Si tratta di misure volte ad evitare false rappresentazioni degli investimenti e dei contratti.</p>		
<i>Procedure per le comunicazioni verso l'esterno (Confindustria)</i>		
<p>I rapporti con la stampa sono gestiti da M&C. Attraverso un comunicato stampa sono trasmessi i dati finanziari della Corporate nei contenuti e con le modalità indicati da quest'ultima.</p>		
<p>I rapporti con le Autorità di Vigilanza (in particolare con l'AGCOM) sono tenuti dal Responsabile TLC che per gli adempimenti relativi collabora con l'ufficio legale e il controlling</p>		
<i>Sistema di deleghe (Confindustria)</i>		
<p>I poteri di firma e le deleghe sono assegnati rispettando la struttura organizzativa e ricorrendo nelle aree più sensibili alla doppia firma. Nei casi in cui è prevista la doppia firma, talvolta è richiesto che una delle due provenga da una funzione determinata (firma obbligatoria). Sono esplicitamente indicate delle soglie di approvazione delle spese e dei livelli di autorizzazione per la stipula dei contratti</p>		
<i>Conservazione e controllo della documentazione aziendale</i>		

<u>DPS/6.2 Contromisure per l'integrità dei dati</u> Si tratta di misure volte a ridurre il rischio di perdita o modifica dei dati personali. Qui rilevano con riferimento all'esigenza di conservare la documentazione aziendale anche su supporto informatico		
<u>DPS/7 Misure di Sicurezza Logiche, Fisiche e Organizzative</u> Si tratta delle misure adottate in adempimento al disciplinare tecnico ex d.lgs. 196/03. Qui rilevano in quanto volte a garantire l'integrità e la disponibilità dei dati		
<u>DPS/7.3.9 Controllo e procedure di controllo accessi agli archivi cartacei</u> Si tratta di misure che disciplinano l'accesso e la disponibilità della documentazione su supporto cartaceo. Qui rilevano per gli aspetti relativi alla conservazione della documentazione (armadi chiusi, contenitori etc.)		
Politica di sicurezza delle Informazioni: <u>Certificazione 27001, SAS 70</u> Qui rileva per garantire l'integrità e la disponibilità dei dati		
<u>Piano di Business Continuity</u> Qui rileva per garantire l'integrità e la disponibilità dei dati		
<u>Piano di Disaster Recovery</u> Qui rileva per garantire l'integrità e la disponibilità dei dati		
<i>Controllo dei sistemi informativi (Confindustria)</i>		
<u>Misure Sox/Information Technology/24000288-24000289-24000290</u> Si tratta di misure volte a garantire la correttezza e il controllo delle transazioni batch e on line e la produzione dei relativi report Qui rilevano per garantire il monitoraggio delle tecnologie utilizzate per la formazione e la trasmissione dei dati economici		
<u>DPS/7.3.4 Sicurezza nella trasmissione dei dati</u> Si tratta di misure volte a proteggere le connessioni di rete Qui rilevano per garantire il monitoraggio delle tecnologie utilizzate per la trasmissione dei dati economici		
Politica di sicurezza delle Informazioni: <u>Certificazione 27001, SAS 70</u> Qui rileva per garantire il monitoraggio dell'utilizzo delle tecnologie utilizzate per la trasmissione dei dati economici		
ILLECITE OPERAZIONI SOCIETARIE		
Indebita restituzione dei conferimenti.	Illegale ripartizione degli utili e delle riserve.	Illecite operazioni sulle azioni o quote sociali o della società controllante.
Operazioni in pregiudizio dei creditori.	Formazione fittizia del capitale.	Indebita ripartizione dei beni sociali da parte dei liquidatori.
<i>Procedure autorizzative per acquisti e vendite di azioni proprie e/o di altre società (Confindustria)</i>		
Procedura per l'acquisizione di rami di azienda. T-Systems può acquisire solo rami di azienda (anche di società quotate) di valore inferiore ad una cifra determinata. L'acquisizione di società terze o di rami di azienda di valore superiore alla cifra detta è rimessa alla decisione della Corporate o in alcuni casi di Deutsche Telekom. L'acquisizione di rami di azienda è un atto di straordinaria amministrazione. L'esame di due diligence è affidata alle funzioni F&C, UL e Personale. In casi complessi intervengono competenze specializzate indicate dalla casa madre		
<u>Misure Sox/Noncurrent assets/all</u> Si tratta di misure volte a documentare e controllare nuovi investimenti, nuovi prestiti, cambi azionari, nuove modifiche normative, e a monitorare perdite e rischi finanziari		
<u>Misure Sox/Sales/all</u> Si tratta di misure volte ad evitare false rappresentazioni degli investimenti e dei contratti.		

Conservazione e controllo della documentazione aziendale

Misure Sox/Treasury/all

Si tratta di procedure volte a garantire che tutti gli items siano calcolati correttamente, che le transazioni finanziarie registrate riflettano circostanze e condizioni economiche reali in accordo con le regole di contabilità e che le riserve siano disposte in modo adeguato

Qui rilevano allo scopo di rendere disponibili tutte le informazioni necessarie ad una corretta gestione delle operazioni societarie

c) Reati con finalità di terrorismo

REATI CON FINALITÀ DI TERRORISMO	
Condotte con finalità di terrorismo (associazione sovversiva, assistenza agli associati, arruolamento, attentato, sequestro, istigazione)	Finanziamento del terrorismo
<i>Controllo sugli investimenti</i>	
<u>Misure Sox/Noncurrent assets/ 24000101-102-103-108-109-114</u> Si tratta di misure volte a documentare e controllare nuovi investimenti, nuovi prestiti, cambi azionari. Qui rilevano per ridurre il rischio che attività finanziarie favoriscano iniziative con finalità di terrorismo	
<u>Procedura per l'acquisizione di rami di azienda</u> T-Systems Italia spa può acquisire solo rami di azienda (anche di società quotate) di valore inferiore ad una cifra determinata. L'acquisizione di società terze o di rami di azienda di valore superiore alla cifra detta è rimessa alla decisione della Corporate o in alcuni casi di Deutsche Telekom. L'acquisizione di rami di azienda è un atto di straordinaria amministrazione. L'esame di due diligence è affidata alle funzioni F&C, UL e Personale. In casi complessi intervengono competenze specializzate indicate dalla casa madre	
<i>Controllo dei sistemi informativi</i>	
<u>Misure Sox/Information Technology/24000288-24000289-24000290</u> Si tratta di misure volte a garantire la correttezza delle transazioni batch e on line e la produzione dei relativi report Qui rilevano per garantire il monitoraggio delle tecnologie utilizzate	
<u>DPS/7.3.4 Sicurezza nella trasmissione dei dati</u> Si tratta di misure volte a proteggere le connessioni di rete Qui rilevano per garantire il monitoraggio delle tecnologie utilizzate	
<u>Politica di sicurezza delle Informazioni: Certificazione 27001, SAS 70</u> Qui rileva per garantire il monitoraggio dell'utilizzo delle tecnologie utilizzate per la trasmissione dei dati economici	

d) Reati contro la persona

REATI CONTRO LA PERSONA		
Riduzione o mantenimento in schiavitù o in servitù	Prostituzione minorile	Pornografia minorile
Iniziative turistiche volte allo sfruttamento della prostituzione minorile	Tratta di persone.	Acquisto e alienazione di schiavi
<i>Esplícita previsione tra i principi etici (Confindustria)</i>		
<u>Codice deontologico di Gruppo</u> Pag. 9 Carta sociale Qui rileva per gli aspetti attinenti i rapporti di lavoro		
<u>Codice Etico Italia</u> 2.4 Tutela della persona Qui rileva per gli aspetti relativi al rispetto della persona nei rapporti tra dipendenti		
<i>Controllo sugli investimenti</i>		
<u>Misure Sox/Noncurrent assets/ 24000101-102-103-108-109-114</u> Si tratta di misure volte a documentare e controllare nuovi investimenti, nuovi prestiti, cambi azionari. Qui rilevano per ridurre il rischio che attività finanziarie favoriscano iniziative che comportino i reati in questione		
Procedura per l'acquisizione di rami di azienda. T-Systems può acquisire solo rami di azienda (anche di società quotate) di valore inferiore ad una cifra determinata. L'acquisizione di società terze o di rami di azienda di valore superiore alla cifra detta è rimessa alla decisione della Corporate o in alcuni casi di Deutsche Telekom. L'acquisizione di rami di azienda è un atto di straordinaria amministrazione. L'esame di due diligence è affidata alle funzioni F&C, UL e Personale. In casi complessi intervengono competenze specializzate indicate dalla casa madre		
<i>Controllo dei sistemi informativi</i>		
<u>Misure Sox/Information Technology/24000288-24000289-24000290</u> Si tratta di misure volte a garantire la correttezza delle transazioni batch e on line e la produzione dei relativi report Qui rilevano per garantire il monitoraggio delle tecnologie utilizzate		
<u>DPS/7.3.4 Sicurezza nella trasmissione dei dati</u> Si tratta di misure volte a proteggere le connessioni di rete Qui rilevano per garantire il monitoraggio delle tecnologie utilizzate		
Politica di sicurezza delle Informazioni: <u>Certificazione 27001, SAS 70</u> Qui rileva per garantire il monitoraggio dell'utilizzo delle tecnologie utilizzate per la trasmissione dei dati economici		
<i>Procedure per viaggi</i>		
Non si prevede il ricorso di viaggi premio per dipendenti e amministratori.		
I viaggi di clienti e giornalisti sono decisi da M&C e sono strettamente correlati ad eventi relativi all'attività dell'azienda o del gruppo.		

e) Reati di abuso di mercato

ABUSI DI MERCATO	
Abuso di informazioni privilegiate	Manipolazione del mercato Qui rilevano le manipolazioni informative e non quelle operative
<i>Esplicita previsione tra i principi etici (Assogestioni)</i>	
<u>Codice deontologico di Gruppo</u> Pag. 14 Conflitto di interessi Pag. 15 Collaborazione con i terzi	
<u>Codice Etico Italia</u> 2.3 Riservatezza e privacy 3.6 Rapporti con gli organi di informazione 3.10 Uso di informazioni interne	
<i>Presidi per garantire la diffusione di informazioni corrette (Assogestioni)</i>	
<u>Misure Sox/ Financial Statements/all</u> Si tratta di misure volte a garantire la produzione e la diffusione corretta delle informazioni finanziarie dell'azienda	
<i>Misure volte a impedire la diffusione di informazioni riservate (Assogestioni)</i>	
Le funzioni coinvolte nell'attività di due diligence (F&C, UL e Direzione Personale) sono tenute alla sottoscrizione di dichiarazione di riservatezza.	
Le informazioni riservate che risiedono nei sistemi informativi dei clienti ospitati sui server di T-Systems sono collocate all'interno delle singole applicazioni, ai quali T-Systems non ha generalmente accesso. Nel caso in cui T-Systems abbia accesso alle applicazioni sono adottate misure organizzative volte a limitare l'accesso alle informazioni solo alle persone che per lo svolgimento delle loro attività ne abbiano necessità. Tra queste, sono previste autorizzazioni diverse per le attività di sviluppo e per quelle di produzione	
<u>DPS/6.3 Contromisure per la Riservatezza dei dati</u> Si tratta di misure volte a garantire l'accesso ai dati personali alle sole persone autorizzate Qui rilevano per ridurre il rischio di accesso ad informazioni finanziarie o economiche riservate	
<u>DPS/7. Misure di Sicurezza Logiche, Fisiche e Organizzative</u> Si tratta delle misure adottate in adempimento al disciplinare tecnico ex d.lgs. 196/03. Qui rilevano in quanto volte a garantire la riservatezza dei dati	
Politica di sicurezza delle Informazioni: <u>Certificazione 27001, SAS 70</u> Qui rilevano in quanto volte a garantire la riservatezza dei dati	
<i>Controllo dei sistemi informativi (Assogestioni)</i>	
<u>Misure Sox/Information Technology/24000288-24000289-24000290</u> Si tratta di misure volte a garantire la correttezza e il controllo delle transazioni batch e on line e la produzione dei relativi report Qui rilevano per garantire il monitoraggio delle tecnologie per l'accesso alle informazioni che risiedono sui server e per la diffusione delle stesse	
<u>DPS/7.3.4 Sicurezza nella trasmissione dei dati</u> Si tratta di misure volte a proteggere le connessioni di rete Qui rilevano per garantire il monitoraggio delle tecnologie per l'accesso alle informazioni che risiedono sui server e per la diffusione delle stesse	
Politica di sicurezza delle Informazioni: <u>Certificazione 27001, SAS 70</u> Qui rilevano per garantire il monitoraggio delle tecnologie per l'accesso alle informazioni che risiedono sui server e per la diffusione delle stesse	

f) Reati transnazionali ex lege 146/06

REATI EX LEGE146/06				
Associazione a delinquere	Riciclaggio	Impiego di denaro, beni o utilità di provenienza illecita	Induzione a non rendere dichiarazioni mendaci all'autorità giudiziaria	Favoreggiamento personale
<i>Misure nei rapporti con i terzi collaboratori</i>				
<u>Misure Sox/Purchasing/24000260-261</u> Si tratta di misure volte a selezionare in modo corretto fornitori e partners Qui rilevano per ridurre il rischio di porre in essere rapporti di collaborazione con soggetti coinvolti nei reati in questione				
<i>Controllo sui flussi finanziari aziendali</i>				
<u>Procedura SAP</u> per gestione acquisti e pagamenti				
Le spese non previste dal budget sono espressamente autorizzate. L'autorizzazione prevede il controllo incrociato del Responsabile dell'area del richiedente e della funzione di Controlling.				
Il Responsabile dell'ordine di acquisto approva il pagamento in modo che sia garantita la verifica dell'esistenza non meramente contabile delle prestazioni effettuate da terzi				
<i>Controllo dei sistemi informativi</i>				
<u>Misure Sox/Information Technology/24000288-24000289-24000290</u> Si tratta di misure volte a garantire la correttezza delle transazioni batch e on line e la produzione dei relativi report Qui rilevano per garantire il monitoraggio dell'uso delle tecnologie				
<u>DPS/7.3.4 Sicurezza nella trasmissione dei dati</u> Si tratta di misure volte a proteggere le connessioni di rete Qui rilevano per garantire il monitoraggio delle tecnologie utilizzate				
Politica di sicurezza delle Informazioni: <u>Certificazione 27001, SAS 70</u> Qui rilevano per garantire il monitoraggio delle tecnologie utilizzate				
<i>Conservazione e controllo della documentazione aziendale</i>				
Procedura che prevede la conservazione della documentazione su supporto cartaceo e su supporto informatico (<u>Livelink</u>) utilizzato da Ufficio Legale, Ufficio Acquisti e segreteria per protocollo della posta				
<u>Misure Sox/Sales/24000118-119-121-122-124-125-127-128-129-130-132-133-607</u> Si tratta di misure volte alla conservazione e aggiornamento delle informazioni relative alle vendite Qui rilevano ai fini di consentire il controllo sulla documentazione relativa allo svolgimento dell'attività di vendita				
<u>DPS/6.2 Contromisure per l'integrità dei dati</u> Si tratta di misure volte a ridurre il rischio di perdita o modifica dei dati personali. Qui rilevano con riferimento all'esigenza di conservare la documentazione aziendale anche su supporto informatico				
<u>DPS/7 Misure di Sicurezza Logiche, Fisiche e Organizzative</u> Si tratta delle misure adottate in adempimento al disciplinare tecnico ex d.lgs. 196/03. Qui rilevano in quanto volte a garantire l'integrità e la disponibilità dei dati				
<u>DPS/7.3.9 Controllo e procedure di controllo accessi agli archivi cartacei</u> Si tratta di misure che disciplinano l'accesso e la disponibilità della documentazione su supporto cartaceo. Qui rilevano per gli aspetti relativi alla conservazione della documentazione (armadi chiusi, contenitori etc.)				
Politica di sicurezza delle Informazioni: <u>Certificazione 27001, SAS 70</u> Qui rileva in quanto volta a garantire l'integrità e la disponibilità dei dati				

Piano di Business Continuity

Qui rileva in quanto volta a garantire l'integrità e la disponibilità dei dati

Piano di Disaster Recovery

Qui rileva in quanto volta a garantire l'integrità e la disponibilità dei dati

g) Omicidio colposo e lesioni colpose gravi

REATI IN MATERIA DI SICUREZZA SUL LAVORO	
Omicidio colposo	Lesioni colpose gravi
<u>Misure di sicurezza ai sensi della legge 626/94</u> T-Systems ha adottato il Sistema di Gestione della Salute e della Sicurezza sul Lavoro che viene allegato 5 al presente Modello	

h) Reati di ricettazione, riciclaggio e impiego di denaro, beni o altra utilità di provenienza illecita

REATI DI RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O ALTRA UTILITA' DI PROVENIENZA ILLECITA		
Ricettazione	Riciclaggio	Impiego di denaro, beni o utilità di provenienza illecita
<i>Esplicita previsione tra i principi etici</i>		
<u>Codice deontologico di gruppo</u> Pag. 15 Riciclaggio Qui rileva limitatamente alla previsione relativa all'adozione di misure volte ad impedire il riciclaggio di denaro		
<i>Misure nei rapporti con i terzi collaboratori</i>		
<u>Misure Sox/Purchasing/24000260-261</u> Si tratta di misure volte a selezionare in modo corretto fornitori e partners Qui rilevano per ridurre il rischio di porre in essere rapporti di collaborazione con soggetti coinvolti nei reati in questione		
<i>Controllo sui flussi finanziari aziendali</i>		
<u>Procedura SAP</u> per gestione acquisti e pagamenti Le spese non previste dal budget sono espressamente autorizzate. L'autorizzazione prevede il controllo incrociato del Responsabile dell'area del richiedente e della funzione di Controlling. Il Responsabile dell'ordine di acquisto approva il pagamento in modo che sia garantita la verifica dell'esistenza non meramente contabile delle prestazioni effettuate da terzi		
<i>Controllo sugli investimenti</i>		
<u>Misure Sox/Noncurrent assets/24000101-102-103-108-109- 114</u> Si tratta di misure volte a documentare e controllare nuovi investimenti, nuovi prestiti, cambi azionari. Qui rilevano per ridurre il rischio che le attività in questione possano celare operazioni di ricettazione, riciclaggio o impiego di denaro di provenienza illecita		
<u>Procedura per l'acquisizione di rami di azienda</u> T-Systems Italia spa può acquisire solo rami di azienda di valore inferiore ad una cifra determinata. L'acquisizione di società terze o di rami di azienda di valore superiore alla cifra detta è rimessa alla decisione della Corporate o in alcuni casi di Deutsche Telekom. L'acquisizione di rami di azienda è un atto di straordinaria amministrazione. L'esame di due diligence è affidata alle funzioni F&C, UL e Personale. In casi complessi intervengono competenze specializzate indicate dalla casa madre		
<i>Misure nei rapporti con i terzi collaboratori</i>		
<u>Misure Sox/Purchasing/2400020- 2400021</u> Le misure sono volte a garantire la corretta selezione dei collaboratori/prestatori di servizi <u>Global Procurement Practices della Corporate</u>		

i) Crimini informatici

CRIMINI INFORMATICI			
Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico	Danneggiamento di informazioni, dati e programmi informatici	Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità	Danneggiamento di sistemi informatici o telematici
Attentato a impianti di pubblica utilità	Falsità in documenti informatici	Accesso abusivo ad un sistema informatico	Detenzione e diffusione abusiva di codici di accesso a sistemi informatici e telematici
<p><u>Certificazione 27001</u> SO/IEC 27001 (ex BS 7799) è una norma che definisce i requisiti per sistemi di gestione della sicurezza delle informazioni. Contribuisce a identificare, gestire e ridurre al minimo la gamma di pericoli a cui sono regolarmente soggette le informazioni. Sono previsti 10 tipi di controllo:</p> <ul style="list-style-type: none"> - Politica di sicurezza: fornisce l'orientamento della gestione e il supporto per la sicurezza delle informazioni - Organizzazione del patrimonio informativo e delle risorse: per aiutarvi a gestire la sicurezza delle informazioni nell'organizzazione - Classificazione e controllo del patrimonio informativo per aiutarvi a identificare il vostro patrimonio informativo e proteggerlo adeguatamente - Sicurezza del personale: per ridurre il rischio di errore umano, furto, frode o uso improprio delle strutture - Sicurezza fisica e ambientale: per prevenire l'accesso non autorizzato, il danneggiamento e le interferenze relativamente ai locali e alle informazioni dell'azienda - Gestione delle comunicazioni e delle operazioni: per assicurare l'utilizzo corretto e sicuro delle strutture di elaborazione delle informazioni - Controllo dell'accesso: per controllare l'accesso alle informazioni - Sviluppo e mantenimento del sistema: per assicurare che la sicurezza sia incorporata nei sistemi informativi - Gestione della continuità aziendale: per contrastare le interruzioni delle attività aziendali e per proteggere le procedure critiche dell'azienda dagli effetti di guasti molto gravi o calamità - Conformità: per evitare violazioni delle leggi penali e civili, degli obblighi di legge, normativi o contrattuali e di qualsiasi requisito relativo alla sicurezza 			
<p><u>SAS 70</u> Lo Statement on Auditing Standards Number 70 (SAS 70) è uno standard per il controllo riconosciuto a livello internazionale dall'American Institute of Certified Public Accountants (AICPA). I SAS 70 sono riconosciuti come controlli di sicurezza approfonditi rivolti ad ambienti di fornitori di servizi, che prevedono controlli sulle reti e relativi processi. L'ultimo audit in T-Systems Italia spa ha avuto esito positivo</p>			
<p><u>Documento Programmatico della Sicurezza</u> Il DPS è il documento redatto in adempimento dell'allegato B del D.Lgs. 196/03 a protezione dei dati personali. E' aggiornato annualmente e descrive le misure di sicurezza (fisiche, logiche e organizzative) a tutela dei dati personali trattati da T-Systems Italia spa.</p>			
<p><u>Misure Sox/Information Technology/</u></p>			

Si tratta delle misure tecnologiche adottate in adempimento del Sarbanes-Oxley act.

Nel corso del 2007 si è dato attuazione ad un progetto sperimentale che, per migliorare le modalità di controllo sull'uso degli strumenti informatici, consentiva di correlare tra loro i log registrati nei vari ambienti. Il progetto consentiva di avere un quadro complessivo e di interpretare le varie correlazioni tra i log in modo da evidenziare eventuali anomalie. Il progetto si è concluso mostrando l'efficacia degli strumenti e delle modalità adottate.

j) Reati di corruzione tra privati

REATI DI CORRUZIONE TRA PRIVATI
I poteri di firma e le deleghe sono assegnati rispettando la struttura organizzativa e ricorrendo nelle aree più sensibili alla doppia firma. Nei casi in cui è prevista la doppia firma, talvolta è richiesto che una delle due provenga da una funzione determinata (firma obbligatoria). Sono esplicitamente indicate delle soglie di approvazione delle spese e dei livelli di autorizzazione per la stipula dei contratti
Procedure per l'acquisizione di beni e servizi mediante aste on line (procedure per eAuction)
<u>Misure Sox/Purchasing/ 24000260-24000261</u> Le misure sono volte a garantire la corretta selezione dei collaboratori/prestatori di servizi. Qui rilevano ai fini della selezione di terzi collaboratori che operano nei rapporti con la PA in modo da ridurre la probabilità che si producano situazioni a rischio corruzione.
<u>Global Procurement Practices della Corporate Purchasing Policy di T-Systems Italia spa</u> (di cui in particolare il <u>Suppliers Management Process (SUM)</u> <u>Procedura SAP</u> <u>Utilizzo della PO Checklist</u> Le misure sono volte a garantire una disciplina certa e trasparente per l'acquisto di beni e servizi. Qui rilevano per garantire trasparenza nella selezione di consulenti (commerciali e non) e fornitori

5. Modello organizzativo

Sulla base delle considerazioni che precedono, tenendo conto:

1. della mappatura dei rischi;
2. delle misure attualmente in essere a contenimento del rischio di reati;
3. di quelle suggerite dagli studi più recenti e dalle indicazioni di Confindustria,

si adotta il Modello che poggia sui seguenti punti:

- codici di comportamento;
- misure a contenimento del rischio di reati;
- Organismo di Vigilanza;
- sistema sanzionatorio;
- piano di formazione e informazione per i dipendenti.

a) Codici di comportamento

I dipendenti di T-Systems sono tenuti al rispetto del codice di comportamento interno dell'azienda e di quello del gruppo. Entrambi i codici definiscono i principi ai quali si ispira l'azienda nello svolgimento dell'attività. Il codice di T-Systems adatta al contesto italiano i principi generali fissati dalla capogruppo.

I testi dei due codici sono stati portati a conoscenza di tutti i dipendenti e sono visionabili in qualsiasi momento sulla intranet aziendale nell'area Corporate Governance.

b) Misure a contenimento del rischio di reati

Si adottano le misure riportate nella seguente tabella ad integrazione di quelle in essere, la cui mappatura è riportata al capitolo 5.

b.1) Reati nei confronti della pubblica amministrazione

REATI DI CORRUZIONE
<i>Sistema di deleghe (Confindustria)</i>
1. Si abbassa la soglia per cui è previsto un sistema a doppia firma per i contratti d'acquisto; 2. Si prevede la firma del CEO e del CFO per la stipula dei contratti di consulenza tecnica o commerciale a favore della pubblica amministrazione in cui sono previsti corrispettivi con una parte variabile. Si precisa che per pubblica amministrazione si intende anche il concessionario di pubblico servizio.
<i>Misure nei rapporti con i terzi collaboratori (Confindustria)</i>
1. Si prevede di adottare nei rapporti con i consulenti clausole contrattuali che impongano vincoli più stringenti al rispetto del codice di condotta di T-Systems e una clausola risolutiva espressa in caso di violazione dello stesso; 2. Si prevede di adottare una procedura che dia attuazione alla disposizione contrattuale che prevede in capo ai consulenti la redazione di un rendiconto puntuale, subordinando il pagamento della prestazione all'approvazione del rendiconto; 3. Si prevede di inserire in contratto una clausola che consenta a T-Systems di esercitare un controllo sull'utilizzo del denaro ricevuto dal consulente in esecuzione del contratto.
<i>Controllo sui flussi finanziari</i>
1. Si decide di formalizzare la procedura già esistente di controllo sui flussi finanziari.
<i>Procedure per omaggi e sponsorizzazioni (Confindustria)</i>
1. Si decide che gli omaggi sono subordinati all'autorizzazione preventiva del Direttore Commerciale; 2. Si decide di fissare un tetto massimo di spesa; 3. Si conferma il divieto presente nel Codice Etico di fornire omaggi a funzionari pubblici
<i>Procedure di assunzione del personale</i>
1. Si decide che l'Ufficio del Personale adotti una procedura volta ad evidenziare eventuali incompatibilità dei candidati relativamente ad eventuali loro rapporti familiari con funzionari pubblici
REATI DI FRODE AI DANNI DELLO STATO
<i>Separazione funzionale tra chi gestisce le attività realizzative e chi presenta la documentazione alla PA (Confindustria)</i>
1. Si decide di rimettere la questione alla valutazione dell'Organismo di Vigilanza 2. Si decide di formalizzare la procedura di gestione delle gare pubbliche
<i>Specifiche attività di controllo gerarchico su documentazione da presentare (relativamente sia alla documentazione di progetto che alla documentazione attestante i requisiti tecnici, economici e professionali dell'azienda che presenta il progetto). (Confindustria)</i>
1. Si decide di formalizzare una procedura che preveda un controllo sulla documentazione prodotta su richiesta del cliente e non espressamente prevista dal contratto
<i>Coerenza delle procure verso l'esterno con il sistema delle deleghe (Confindustria)</i>
1. Si decide che all'atto della stipula di contratti con terzi, chi ha poteri di firma fornisca all'altra parte copia in carta semplice della procura.
<i>Procedure per omaggi e sponsorizzazioni (Confindustria)</i>
1. Si decide che gli omaggi sono subordinati all'autorizzazione preventiva del Direttore Commerciale; 2. Si decide di fissare un tetto massimo di spesa; 3. Si conferma il divieto presente nel Codice Etico di fornire omaggi a funzionari pubblici

b.2) Reati societari

FALSE COMUNICAZIONI SOCIALI
<i>Esplicita previsione tra i principi etici (Confindustria)</i>
1. Si decide di introdurre nel Codice Etico di T-Systems una disposizione volta a sollecitare la comunicazione di informazioni tempestive, corrette e veritiere agli organi interni deputati alla redazione del bilancio e della documentazione economica aziendale in genere
<i>Procedura rivolta alle funzioni aziendali con cui si stabiliscono le modalità per garantire la produzione delle informazioni di bilancio e la corretta trasmissione delle stesse agli organi deputati (Confindustria)</i>
1. Si decide di corredare la trasmissione da parte dei vari responsabili delle informazioni di bilancio da una dichiarazione con cui essi attestano la diligenza con cui le informazioni sono state prodotte. 2. Si decide di formalizzare la procedura già esistente che prevede la tempestiva messa a disposizione di tutti i componenti del Consiglio di Amministrazione della bozza del bilancio e del giudizio dei revisori, prima della riunione del Consiglio di Amministrazione di approvazione dello stesso (con documentazione attestante l'avvenuta consegna); 3. Si decide di formalizzare la procedura già esistente che prevede la sottoscrizione del CEO della lettera di attestazione o manleva richiesta dai revisori, unitamente alla sigla del CFO ed alla messa a disposizione del Consiglio di Amministrazione
<i>Procedure per le comunicazioni verso l'esterno (Confindustria)</i>
1. Si decide di attribuire la responsabilità della gestione dei rapporti con l'Agcom (Autorità per le Garanzie nelle Comunicazioni) al responsabile TLC, unitamente al confezionamento di apposita reportistica al CEO.

b.3) Reati con finalità di terrorismo

REATI CON FINALITÀ DI TERRORISMO
<i>Controllo sugli investimenti</i>
1. Si decide di adottare nel corso dell'attività di due diligence per l'acquisizione di rami di azienda il ricorso a black list.

b.4) Reati contro la persona

REATI CONTRO LA PERSONA
<i>Controllo sugli investimenti</i>
1. Si decide di adottare nel corso dell'attività di due diligence per l'acquisizione di rami di azienda il ricorso a black list.
<i>Procedure per viaggi</i>
1. Si decide di adottare una procedura formalizzata in materia di viaggi premio per dipendenti e collaboratori. 2. Si decide di formalizzare le regole di comportamento già in uso nell'organizzazione degli eventi; 3. Si decide di adottare una procedura che riconosce a M&C il controllo sulle spese di viaggio per i clienti secondo criteri predefiniti.

b.5) Reati di abuso di mercato

ABUSI DI MERCATO
<i>Misure volte a impedire la diffusione di informazioni riservate (Assogestioni)</i>
1. Si decide di inserire una clausola di "non disclosure" in tutti i contratti con i collaboratori 2. Si decide adottare una procedura che individui in modo puntuale i gradi di riservatezza delle informazioni e le modalità di trattamento delle stesse; 3. Si decide di formalizzare i controlli già operativi per evitare nell'ambito di procedure pubbliche cartelli con monopolisti o soggetti che forniscono servizi in esclusiva

b.6) Reati transnazionali ex lege 146/06

REATI EX LEGE146/06
<i>Esplícita previsione tra i principi etici</i>
1. Si decide di inserire nel Codice Etico di T-Systems una disposizione volta a garantire la trasparenza nei rapporti con l'Autorità giudiziaria.
<i>Controllo sui flussi finanziari aziendali</i>
1. Si decide di formalizzare la procedura già esistente per l'autorizzazione di spese.

b.7) Reati in materia di sicurezza sul lavoro

OMICIDIO COLPOSO, LESIONI GRAVI O GRAVISSIME

1. Si decide di adottare una procedura più stringente nel caso di lavori di trasloco, ristrutturazione etc. che coinvolgano i locali dell'azienda

b.8) Reati di ricettazione, riciclaggio e impiego di denaro, beni e altre utilità di provenienza illecita

RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI E ALTRE UTILITÀ DI PROVENIENZA ILLECITA

Controllo sui flussi finanziari

Si decide di formalizzare la procedura già esistente per l'autorizzazione di spesa

Misure nei rapporti con i terzi collaboratori

1. Si prevede di adottare una procedura che dia attuazione alla disposizione contrattuale che prevede in capo ai consulenti la redazione di un rendiconto puntuale, subordinando il pagamento della prestazione all'approvazione del rendiconto
2. Si prevede di inserire in contratto una clausola che consenta a T-Systems di esercitare un controllo sull'utilizzo del denaro ricevuto dal consulente in esecuzione del contratto
3. Si decide di adottare una procedura di verifica del coinvolgimento di persone politicamente esposte

Controllo sugli investimenti

1. Si decide di ricorrere a black list nel corso dell'attività di due diligence per l'acquisizione di rami di azienda
2. Si decide di adottare nel corso dell'attività di due diligence una procedura di verifica del coinvolgimento di persone politicamente esposte

b.9) Crimini informatici

CRIMINI INFORMATICI

Da valutare l'opportunità di passare dalla sperimentazione (attuata lo scorso anno) all'implementazione delle procedure di correlazione tra i log di vari ambienti

Reati di corruzione tra privati

REATI DI CORRUZIONE TRA PRIVATI

1. Si introduce un sistema a doppia firma per i contratti d'acquisto.

b.10) Appendice su Advisory Board

Si decide di integrare il redigendo Statuto dell'Advisory Board con richiami espliciti al codice di comportamento del Gruppo e di T-Systems e a vincoli di riservatezza e di confidenzialità.

c) Organismo di Vigilanza

c.1) Indipendenza

L'Organismo di Vigilanza è nominato dal Consiglio di Amministrazione. I componenti dell'Organismo di Vigilanza debbono essere, almeno in prevalenza, personale interno all'impresa, ed al contempo debbono possedere capacità specifiche in tema di attività ispettiva e consulenziale.

Non possono essere nominati nell'Organismo di Vigilanza persone che abbiano subito sentenze di condanna (o di patteggiamento) per qualsiasi tipo di reato. Il Consiglio di Amministrazione provvede alla revoca qualora i componenti dell'OdV siano imputati in procedimenti penali e in caso di sopravvenuta ed assoluta incapacità, incompatibilità o negligenza nello svolgimento dell'incarico. La delibera di revoca è portata a conoscenza e sottoposta al previo assenso del Collegio Sindacale.

Tale organismo è ritenuto idoneo in quanto fornito dei requisiti personali di autonomia, indipendenza, professionalità, continuità di azione, di capacità specifiche in tema di attività ispettiva e consulenziale, nonché dei mezzi organizzativi necessari per l'esercizio della specifica funzione.

In particolare il requisito dell'autonomia si evidenzia nella collocazione organizzativa aziendale dell'OdV che risponde direttamente al Consiglio di Amministrazione. L'indipendenza dell'OdV è assicurata dalla presenza all'interno di quest'ultimo di un soggetto esterno all'organigramma aziendale.

L'OdV viene nominato dal Consiglio di Amministrazione unitamente alla approvazione del presente Modello.

c.2) Risorse

Sempre al fine di garantire il maggior grado di indipendenza possibile è assegnata annualmente all'OdV, dietro proposta dell'OdV stesso, una dotazione patrimoniale adeguata allo svolgimento dei compiti assegnatigli.

Le spese di carattere straordinario potranno essere autorizzate dal Consiglio di Amministrazione dietro richiesta motivata dell'OdV. In caso di diniego la questione è sottoposta al Collegio sindacale affinché prenda le decisioni opportune.

c.3) Composizione - Durata

L'Organismo di Vigilanza è composto da un minimo di tre membri fino ad un massimo di cinque, di cui almeno un membro è esterno; per l'attuale composizione si veda l'Allegato 4.

La durata in carica dei componenti l'OdV è equiparata a quella del Consiglio di Amministrazione.

Il Consiglio di Amministrazione di T-Systems può revocare in ogni momento i membri dell'OdV in presenza dell'avveramento di una o più cause sopraindicate al punto "Indipendenza".

In caso di rinuncia, di sopravvenuta incapacità, revoca o decadenza di un membro dell'OdV, quest'ultimo ne darà tempestiva comunicazione al Consiglio di Amministrazione il quale provvederà senza indugio alla sua sostituzione.

E' fatto obbligo a ciascun membro dell'OdV di comunicare tempestivamente al Consiglio di Amministrazione il verificarsi di una delle ipotesi dalle quali derivi la necessità di sostituire un membro dell'OdV.

c.4) Competenze

All'Organismo di Vigilanza sono attribuiti in generale i seguenti compiti:

1. verificare l'adeguatezza del Modello adottato, proponendo agli amministratori gli eventuali aggiornamenti qualora le analisi operate rendano necessario effettuare correzioni ed adeguamenti;
2. proporre al Consiglio di Amministrazione:
 - a. la tipologia di informazioni necessarie allo svolgimento dell'attività dell'OdV e le modalità con cui si realizza il flusso di tali informazioni (su richiesta, ad intervalli regolari etc.);
 - b. le modalità con cui amministratori, dipendenti e collaboratori riferiscono all'OdV di comportamenti illeciti di cui siano a conoscenza o segnalano eventuali criticità;
3. esercitare il controllo sul rispetto delle misure adottate a contenimento del rischio di reati individuando le modalità, anche a campione, con cui procedere. L'OdV sarà tenuto ad adottare modalità di controllo stringente per le fattispecie che dalla mappatura dei rischi risultino a probabilità elevata di rischio;
4. segnalare agli amministratori eventuali comportamenti contrari alle procedure previste dal Modello e dal Codice Etico per l'applicazione delle relative sanzioni disciplinari o per la risoluzione del contratto nel caso di collaboratori esterni;
5. segnalare al Collegio Sindacale eventuali comportamenti degli amministratori contrari alle procedure previste dal Modello e dal Codice Etico, perchè provveda alla comunicazione all'assemblea;
6. denunciare alle autorità competenti eventuali reati di cui venisse a conoscenza nell'esercizio delle sue funzioni;

Su un piano più specificatamente operativo all'OdV sono altresì affidati i seguenti compiti:

1. attivare le procedure di controllo previste dal Modello restando precisato che in ogni caso le attività di controllo sono demandate alla responsabilità primaria del management operativo e sono considerate parte integrante di ogni processo aziendale;
2. effettuare ricognizioni dell'attività aziendale ai fini dell'aggiornamento della mappatura delle aree di attività a rischio nell'ambito del contesto aziendale;

- 3 coordinarsi con le altre funzioni aziendali per il monitoraggio delle attività nelle aree a rischio prevedendo lo svolgimento periodico di controlli di routine e di controlli a sorpresa nei confronti delle attività aziendali sensibili, effettuando specifici approfondimenti, analisi e controlli sulle procedure esistenti, sugli atti societari e sui contratti di maggior rilevanza nelle aree di attività a rischio;
- 4 raccogliere, elaborare e conservare le informazioni rilevanti in funzione del rispetto del Modello, nonché aggiornare la lista delle informazioni che devono essere obbligatoriamente trasmesse all'OdV o tenute a sua disposizione;
- 5 controllare l'effettiva presenza e la regolare tenuta ed efficacia della documentazione richiesta in relazione a quanto previsto nel Modello per le diverse tipologie di reato;

c.5) Attività di reporting dell'OdV

L'OdV ha due linee di reporting:

- su base continuativa verso l'Amministratore Delegato ed il Presidente del Collegio Sindacale;
- almeno su base semestrale verso il Consiglio di Amministrazione ed il Collegio Sindacale.

Degli incontri verrà redatto verbale e copia dei verbali verrà custodita dall'OdV e dagli organismi interessati.

Sarà cura dell'OdV preparare almeno due volte l'anno un rapporto scritto sulla sua attività per il Consiglio di Amministrazione e per il Collegio Sindacale, nonché un piano delle attività previste per il semestre successivo.

L'OdV si coordinerà con le funzioni aziendali competenti per i diversi profili specifici e, in particolare, ma non esclusivamente con la Direzione Risorse Umane e la Direzione Legale.

c.6) Reporting verso l'OdV

I dipendenti, i dirigenti e gli amministratori di T-Systems hanno l'obbligo di riferire all'OdV ogni notizia rilevante relativa a violazioni del Modello che possono portare alla commissione di reati o relativi al tentativo di commissione di reati della quale dovessero venire a conoscenza.

Le comunicazioni potranno essere effettuate, anche in forma anonima, utilizzando l'indirizzo e-mail dell'OdV (organo.vigilanza@t-systems.it).

L'OdV non è tenuto a prendere in considerazione le segnalazioni anonime che appaiono prima facie irrilevanti, destituite di fondamento o non circostanziate.

L'omessa comunicazione di informazioni rilevanti potrà essere sanzionata secondo quanto previsto dal presente Modello.

c.7) Raccolta e conservazione delle informazioni

Ogni informazione, segnalazione, report previsti nel presente Modello sono conservati dall'OdV in un apposito Data Base (informatico e/o cartaceo) per un periodo di almeno 5 (cinque) anni.

L'accesso al Data Base è consentito esclusivamente all'OdV, al Collegio Sindacale, agli Amministratori Esecutivi ed al personale delegato dall'OdV.

Segue un elenco esemplificativo delle informazioni da conservarsi nel Data Base:

1. ogni informazione utile riguardante le decisioni relative la richiesta , erogazione ed utilizzo di finanziamenti pubblici;
2. i prospetti riepilogativi degli appalti dei quali T-Systems è risultata aggiudicataria a seguito di gare a livello nazionale ed internazionale ovvero a trattativa privata;
3. le notizie e la documentazione relative ad appalti affidati da enti pubblici o soggetti che svolgono funzioni di pubblica utilità;
4. le richieste di assistenza legale inoltrate da dirigenti, dipendenti o altri soggetti che ne avessero titolo, nei confronti dei quali la magistratura abbia avviato procedimenti per i reati previsti dal D. Lgs. 231/01;
5. i provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti per i reati di cui D. Lgs. 231/01;
6. le notizie relative al rispetto, a tutti i livelli aziendali, del Modello, con evidenza dei procedimenti disciplinari avviati e delle eventuali sanzioni erogate ovvero dei provvedimenti di archiviazione, con le relative motivazioni;
7. i rapporti preparati dai responsabili di altre funzioni aziendali nell'ambito della loro attività di controllo e dai quali possono emergere fatti, atti, eventi o omissioni rilevanti ai sensi del D. Lgs. 231/01;
8. il sistema di deleghe di T-Systems;
9. periodicamente l'OdV proporrà, se del caso, all'Amministratore Delegato eventuali modifiche della lista sopra indicata.

d) Sistema sanzionatorio

I comportamenti contrari

- alle norme dell'ordinamento;
- al codice di comportamento;
- alle procedure prescritte nel Modello;
- alle misure di sicurezza sul lavoro adottate;

si intendono pregiudizievoli dell'interesse dell'azienda. Si considera tale anche la violazione degli obblighi di informazione all'OdV e il comportamento degli amministratori che per negligenza o imperizia non abbiano saputo individuare e quindi eliminare eventuali violazioni di legge, del codice di comportamento o delle procedure prescritte dal Modello.

La sanzione sarà commisurata alla gravità dell'inflazione ed all'eventuale reiterazione della stessa; della recidività si terrà altresì conto anche ai fini della combinazione della sanzione consistente nell'espulsione.

Una errata interpretazione dei principi e delle regole stabiliti dal Modello potrà costituire esimente soltanto nei casi di comportamento di buona fede in cui i vincoli posti dal Modello dovessero eccedere i limiti di approfondimento richiesti ad una persona di buona diligenza.

Tali comportamenti determinano:

d.1) Per i dipendenti

Verranno applicate le sanzioni disciplinari previste dal contratto collettivo nel rispetto delle procedure stabilite dall'art. 7 dello Statuto dei Lavoratori. La sanzione viene applicata dall'Amministratore Delegato o dalla direzione aziendale a cui sono conferiti i relativi poteri su segnalazione dell'OdV.

In applicazione del principio di correlazione tra le mancanze dei lavoratori e i provvedimenti disciplinari si stabilisce che i comportamenti sono sanzionati a seconda del rilievo che assumono le singole fattispecie considerate e le sanzioni in concreto previste per la commissione dei fatti stessi e sono ponderate e proporzionate in base alla loro gravità e all'eventuale loro reiterazione, distinguendosi in ordine crescente, tra:

- richiamo verbale
- rimprovero scritto;
- attribuzione ad altra funzione aziendale, purché ciò non comporti un demansionamento del dipendente;
- sospensione dal servizio e dalla retribuzione per un massimo di dieci giorni;
- licenziamento con preavviso;
- licenziamento senza preavviso.

Prima dell'adozione di qualsiasi provvedimento disciplinare nei confronti del lavoratore a questi sarà contestato l'addebito e lo stesso sarà sentito a sua difesa.

Ad eccezione del richiamo verbale tutte le contestazioni avverranno per iscritto e i provvedimenti disciplinari non potranno essere applicati prima che siano trascorsi 5 (cinque) giorni nel corso dei quali il lavoratore potrà presentare le sue giustificazioni.

L'adozione del provvedimento sarà anch'essa motivata e comunicata per iscritto.

d.2) Per gli Amministratori

In caso di violazione del Modello l'OdV ne darà immediata comunicazione al Consiglio di Amministrazione ed al Collegio Sindacale i quali adotteranno i provvedimenti del caso nell'ambito delle rispettive attribuzioni, ivi compresa l'eventuale convocazione dell'Assemblea con la proposta di eventuale revoca della carica.

Le relative comunicazioni saranno indirizzate direttamente a tutti i componenti del Consiglio di Amministrazione e del Collegio Sindacale con esclusione dei soggetti coinvolti.

d.3) Per i Sindaci

In caso di violazione del Modello l'OdV ne darà immediata comunicazione al Consiglio di Amministrazione ed al Collegio Sindacale i quali adotteranno i provvedimenti del caso nell'ambito delle rispettive attribuzioni, ivi compresa l'eventuale convocazione dell'Assemblea con la proposta di eventuale revoca della carica.

Le relative comunicazioni saranno indirizzate direttamente a tutti i componenti del Consiglio di Amministrazione e del Collegio Sindacale con esclusione dei soggetti coinvolti.

d.4) Per l'Organismo di Vigilanza

In caso di violazione del presente Modello da parte di uno o più membri dell'OdV, gli altri membri ovvero uno qualsiasi tra i Sindaci o tra gli Amministratori informerà immediatamente il Collegio Sindacale ed il Consiglio di Amministrazione i quali prenderanno gli opportuni provvedimenti tra cui, ad esempio, la revoca dell'incarico ai membri dell'OdV che hanno violato il modello e la conseguente nomina di nuovi membri in sostituzione degli stessi, ovvero la revoca dell'incarico all'intero organo e la conseguente nomina di un nuovo OdV.

d.5) Per i partner, consulenti e fornitori

La facoltà di risolvere il contratto. La violazione delle norme dell'ordinamento, del codice di comportamento e, se applicabili, delle procedure prescritte dal Modello organizzativo e delle misure di sicurezza del lavoro è causa di risoluzione del contratto che la prevede quale clausola risolutiva espressa.

Resta salvo ogni diritto della società in ordine ad eventuali azioni risarcitorie per i danni ad essa cagionati dal dipendente, dal dirigente o dal collaboratore a seguito della violazione sia delle procedure che delle norme comportamentali prescritte dal Modello.

e) Piano di formazione

Il piano di formazione è adottato nella consapevolezza che i modelli organizzativi si dimostrano efficaci solo qualora siano conosciuti all'interno dell'azienda e fatti propri da ciascuno.

Si decide di ricorrere a un intervento di formazione destinato a tutti i dipendenti e collaboratori. Il piano prevede l'illustrazione del d.lgs. 231/01 e delle problematiche organizzative che essa pone all'interno dell'azienda; la descrizione del Modello adottato con particolare attenzione alle procedure e al Codice Etico.

Il piano di formazione è realizzato dalla Direzione Risorse Umane in collaborazione con L'OdV e con i responsabili delle altre funzioni di volta in volta coinvolte nell'applicazione del Modello.

L'attività di formazione, è differenziata nei contenuti e nelle modalità di attuazione in funzione della qualifica dei destinatari, del livello di rischio dell'area in cui questi operano, dello svolgimento da parte degli stessi di funzioni di rappresentanza della società e dell'attribuzione di eventuali poteri.

In particolare, sono previsti specifici programmi di formazione relativamente a:

- management;
- componenti dell'OdV;
- dipendenti che operano in specifiche aree di rischio;
- altri dipendenti.

Tutti i programmi di formazione avranno un contenuto minimo comune consistente nell'illustrazione dei principi del D. Lgs. 231/01, degli elementi costitutivi il Modello, delle singole fattispecie di reato e dei comportamenti considerati sensibili in relazione al compimento dei sopra citati reati.

In aggiunta a questa matrice comune ogni programma di formazione sarà modulato al fine di fornire ai suoi fruitori gli strumenti necessari per il pieno rispetto del D. Lgs. 231/01 in relazione all'ambito di operatività ed alle mansioni dei soggetti destinatari del programma stesso.

E' prevista anche la possibilità di ricorrere a modalità di formazione a distanza degli interessati.

La partecipazione ai programmi di formazione è obbligatoria e il controllo è demandato all'OdV.

Brevi cenni sul programma del corso

Il corso sarà composto dai seguenti moduli:

- 1) Breve introduzione alla normativa e ai modelli organizzativi
 - a. La responsabilità dell'impresa;
 - b. Il ruolo dei modelli organizzativi (a cosa servono a chi sono destinati);
 - c. Il contenuto dei Modello di T-Systems.

- 2) I codici di comportamento del gruppo e di T-Systems Italia

- a. Le prescrizioni e la loro funzione nell'ambito dei modelli.
- 3) L'Organismo di Vigilanza di T-Systems Italia
- a. La composizione;
 - b. Le competenze;
 - c. Le relazioni con dipendenti, dirigenti, collaboratori ed amministratori.
- 4) Le procedure a contenimento del rischio di reato
- a. Le procedure che disciplinano l'attività dell'azienda come modalità di contenimento del rischio di reato;
 - b. Le categorie di rischio e le misure adottate.
- 5) Il sistema sanzionatorio

Il piano di formazione prevede via via aggiornamenti anche a seguito delle modifiche ed integrazioni al modello organizzativo che l'Organismo di Vigilanza vorrà adottare e del turn over interno.

f) Piano di informazione

Viene data informazione a tutti i dipendenti e collaboratori dell'adozione del presente Modello fornendo loro, anche attraverso la intranet aziendale:

- un documento estratto dal Modello che descriva le principali novità;
- il codice deontologico;
- le procedure amministrative ed informatiche rilevanti;
- un quadro del sistema sanzionatorio.

La documentazione suddetta verrà fornita anche all'atto dell'assunzione di un nuovo dipendente o all'instaurarsi di un nuovo rapporto di collaborazione.

Il piano di informazione è realizzato dalla Direzione Risorse Umane in collaborazione con L'OdV e con i responsabili delle altre funzioni di volta in volta coinvolte nell'applicazione del Modello.

Allegato 1: “Elenco dei reati”

Reati rilevanti ai sensi del d.lgs. 231/01

Reati contro la pubblica amministrazione

Articoli Codice Penale	
316-bis. Malversazione a danno dello Stato.	Chiunque, estraneo alla pubblica amministrazione, avendo ottenuto dallo Stato o da altro ente pubblico o dalle Comunità europee contributi, sovvenzioni o finanziamenti destinati a favorire iniziative dirette alla realizzazione di opere od allo svolgimento di attività di pubblico interesse, non li destina alle predette finalità, è punito con la reclusione da sei mesi a quattro anni.
316-ter. Indebita percezione di erogazioni a danno dello Stato.	Salvo che il fatto costituisca il reato previsto dall'articolo 640-bis, chiunque mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o attestanti cose non vere, ovvero mediante l'omissione di informazioni dovute, consegue indebitamente, per sé o per altri, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati dallo Stato, da altri enti pubblici o dalle Comunità europee è punito con la reclusione da sei mesi a tre anni. Quando la somma indebitamente percepita è pari o inferiore a lire sette milioni settecentoquarantacinquemila si applica soltanto la sanzione amministrativa del pagamento di una somma di denaro da dieci a cinquanta milioni di lire. Tale sanzione non può comunque superare il triplo del beneficio conseguito.
640. Truffa.	Chiunque, con artifici o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da lire centomila a due milioni. La pena è della reclusione da uno a cinque anni e della multa da lire seicentomila a tre milioni: 1. se il fatto è commesso a danno dello Stato o di un altro ente pubblico o col pretesto di far esonerare taluno dal servizio militare (...)
640-bis. Truffa aggravata per il conseguimento di erogazioni pubbliche	La pena è della reclusione da uno a sei anni e si procede d'ufficio se il fatto di cui all'articolo 640 riguarda contributi, finanziamenti, mutui agevolati ovvero altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati da parte dello Stato, di altri enti pubblici o delle Comunità europee
640-ter. Frode informatica.	Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da lire centomila a due milioni. La pena è della reclusione da uno a cinque anni e della multa da lire seicentomila a tre milioni se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema. Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo comma o un'altra circostanza aggravante
317. Concussione.	Il pubblico ufficiale o l'incaricato di un pubblico servizio, che, abusando della sua qualità o dei suoi poteri costringe o induce taluno a dare o a promettere indebitamente, a lui o ad un terzo, denaro o altra utilità, è punito con la reclusione da quattro a dodici anni

318. Corruzione per un atto d'ufficio.	Il pubblico ufficiale, che, per compiere un atto del suo ufficio, riceve, per sé o per un terzo, in denaro od altra utilità, una retribuzione che non gli è dovuta, o ne accetta la promessa, è punito con la reclusione da sei mesi a tre anni. Se il pubblico ufficiale riceve la retribuzione per un atto d'ufficio da lui già compiuto, la pena è della reclusione fino a un anno
319. Corruzione per un atto contrario ai doveri d'ufficio.	Il pubblico ufficiale che, per omettere o ritardare o per aver omesso o ritardato un atto del suo ufficio, ovvero per compiere o per aver compiuto un atto contrario ai doveri di ufficio, riceve, per sé o per un terzo, denaro od altra utilità, o ne accetta la promessa, è punito con la reclusione da due a cinque anni
319-bis. Circostanze aggravanti.	La pena è aumentata se il fatto di cui all'art. 319 ha per oggetto il conferimento di pubblici impieghi o stipendi o pensioni o la stipulazione di contratti nei quali sia interessata l'amministrazione alla quale il pubblico ufficiale appartiene
319-ter. Corruzione in atti giudiziari	Se i fatti indicati negli articoli 318 e 319 sono commessi per favorire o danneggiare una parte in un processo civile, penale o amministrativo, si applica la pena della reclusione da tre a otto anni. Se dal fatto deriva l'ingiusta condanna di taluno alla reclusione non superiore a cinque anni, la pena è della reclusione da quattro a dodici anni; se deriva l'ingiusta condanna alla reclusione superiore a cinque anni o all'ergastolo, la pena è della reclusione da sei a venti anni
321. Pene per il corruttore.	Le pene stabilite nel primo comma dell'articolo 318, nell' articolo 319, nell' articolo 319-bis, nell' art. 319-ter, e nell' articolo 320 in relazione alle suddette ipotesi degli articoli 318 e 319, si applicano anche a chi dà o promette al pubblico ufficiale o all'incaricato di un pubblico servizio il denaro od altra utilità
322. Istigazione alla corruzione.	Chiunque offre o promette denaro od altra utilità non dovuti ad un pubblico ufficiale o ad un incaricato di un pubblico servizio che riveste la qualità di pubblico impiegato, per indurlo a compiere un atto del suo ufficio, soggiace, qualora l'offerta o la promessa non sia accettata, alla pena stabilita nel primo comma dell'articolo 318, ridotta di un terzo. Se l'offerta o la promessa è fatta per indurre un pubblico ufficiale o un incaricato di un pubblico servizio ad omettere o a ritardare un atto del suo ufficio, ovvero a fare un atto contrario ai suoi doveri, il colpevole soggiace, qualora l'offerta o la promessa non sia accettata, alla pena stabilita nell'articolo 319, ridotta di un terzo. La pena di cui al primo comma si applica al pubblico ufficiale o all'incaricato di un pubblico servizio che riveste la qualità di pubblico impiegato che sollecita una promessa o dazione di denaro od altra utilità da parte di un privato per le finalità indicate dall'articolo 318. La pena di cui al secondo comma si applica al pubblico ufficiale o all'incaricato di un pubblico servizio che sollecita una promessa o dazione di denaro od altra utilità da parte di un privato per le finalità indicate dall'articolo 319
453. Falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate.	E' punito con la reclusione da tre a dodici anni e con la multa da lire un milione a sei milioni : 1. chiunque contraffà monete nazionali [c.p. 458] o straniere, aventi corso legale nello Stato o fuori; 2. chiunque altera in qualsiasi modo monete genuine, col dare ad esse l'apparenza di un valore superiore; 3. chiunque, non essendo concorso nella contraffazione o nell'alterazione, ma di concerto con chi l'ha eseguita ovvero con un intermediario, introduce nel territorio dello Stato [c.p. 4] o detiene o spende o mette altrimenti in circolazione monete contraffatte o alterate; 4. chiunque, al fine di metterle in circolazione, acquista o comunque riceve, da chi le ha falsificate, ovvero da un intermediario, monete contraffatte o alterate.
454. Alterazione di monete.	Chiunque altera monete della qualità indicata nell'articolo precedente, scemandone in qualsiasi modo il valore, ovvero, rispetto alle monete in tal modo alterate, commette alcuno dei fatti indicati nei n. 3 e 4 del detto articolo, è punito con la reclusione da uno a cinque anni e con la multa da lire duecentomila a un milione
455. Spendita e introduzione nello Stato, senza concerto, di monete falsificate.	Chiunque, fuori dei casi preveduti dai due articoli precedenti, introduce nel territorio dello Stato [c.p. 4], acquista o detiene monete [c.p. 458] contraffatte o alterate, al fine di metterle in circolazione, ovvero le spende o le mette altrimenti in circolazione, soggiace alle pene stabilite nei detti articoli, ridotte da un terzo alla metà
457. Spendita di monete falsificate ricevute in buona fede.	Chiunque spende, o mette altrimenti in circolazione monete contraffatte o alterate, da lui ricevute in buona fede, è punito con la reclusione fino a sei mesi o con la multa fino a lire due milioni

<p>459. Falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati.</p>	<p>Le disposizioni degli articoli 453, 455 e 457 si applicano anche alla contraffazione o alterazione di valori di bollo e alla introduzione nel territorio dello Stato [c.p. 4], o all'acquisto, detenzione e messa in circolazione di valori di bollo contraffatti; ma le pene sono ridotte di un terzo [c.p. 63]. Agli effetti della legge penale, si intendono per valori di bollo la carta bollata, le marche da bollo, i francobolli e gli altri valori equiparati a questi da leggi speciali</p>
<p>460. Contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo.</p>	<p>Chiunque contraffà la carta filigranata che si adopera per la fabbricazione delle carte di pubblico credito [c.p. 458] o dei valori di bollo [c.p. 459], ovvero acquista, detiene o aliena tale carta contraffatta, è punito, se il fatto non costituisce un più grave reato, con la reclusione da due a sei anni e con la multa da lire seicentomila a due milioni</p>
<p>461. Fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata.</p>	<p>Chiunque fabbrica, acquista, detiene o aliena filigrane, programmi informatici o strumenti destinati esclusivamente alla contraffazione o alterazione di monete [c.p. 458], di valori di bollo [c.p. 459] o di carta filigranata è punito, se il fatto non costituisce un più grave reato, con la reclusione da uno a cinque anni e con la multa da lire duecentomila a un milione [c.p. 28, 29, 32, 463, 464] La stessa pena si applica se le condotte previste dal primo comma hanno ad oggetto ologrammi o altri componenti della moneta destinati ad assicurare la protezione contro la contraffazione o l'alterazione</p>
<p>464. Uso di valori di bollo contraffatti o alterati.</p>	<p>Chiunque, non essendo concorso nella contraffazione o nell'alterazione, fa uso di valori di bollo [c.p. 459] contraffatti o alterati è punito con la reclusione fino a tre anni e con la multa fino a lire un milione Se i valori sono stati ricevuti in buona fede, si applica la pena stabilita nell'articolo 457, ridotta di un terzo</p>

Reati societari

Articoli Codice Civile	
<p>2621. False comunicazioni sociali.</p>	<p>Salvo quanto previsto dall'articolo 2622, gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, i quali, con l'intenzione di ingannare i soci o il pubblico e al fine di conseguire per sé o per altri un ingiusto profitto, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, espongono fatti materiali non rispondenti al vero ancorché oggetto di valutazioni ovvero omettono informazioni la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene, in modo idoneo ad indurre in errore i destinatari sulla predetta situazione, sono puniti con l'arresto fino a due anni.</p> <p>La punibilità è estesa anche al caso in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi.</p> <p>La punibilità è esclusa se le falsità o le omissioni non alterano in modo sensibile la rappresentazione della situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene. La punibilità è comunque esclusa se le falsità o le omissioni determinano una variazione del risultato economico di esercizio, al lordo delle imposte, non superiore al 5 per cento o una variazione del patrimonio netto non superiore all'1 per cento.</p> <p>In ogni caso il fatto non è punibile se conseguenza di valutazioni estimative che, singolarmente considerate, differiscono in misura non superiore al 10 per cento da quella corretta.</p> <p>Nei casi previsti dai commi terzo e quarto, ai soggetti di cui al primo comma sono irrogate la sanzione amministrativa da dieci a cento quote e l'interdizione dagli uffici direttivi delle persone giuridiche e delle imprese da sei mesi a tre anni, dall'esercizio dell'ufficio di amministratore, sindaco, liquidatore, direttore generale e dirigente preposto alla redazione dei documenti contabili societari, nonché da ogni altro ufficio con potere di rappresentanza della persona giuridica o dell'impresa</p>
<p>2622. False comunicazioni sociali in danno della società, dei soci o dei creditori.</p>	<p>Gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, i quali, con l'intenzione di ingannare i soci o il pubblico e al fine di conseguire per sé o per altri un ingiusto profitto, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, esponendo fatti materiali non rispondenti al vero ancorché oggetto di valutazioni, ovvero omettendo informazioni la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene, in modo idoneo ad indurre in errore i destinatari sulla predetta situazione, cagionano un danno patrimoniale alla società, ai soci o ai creditori, sono puniti, a querela della persona offesa, con la reclusione da sei mesi a tre anni.</p> <p>Si procede a querela anche se il fatto integra altro delitto, ancorché aggravato, a danno del patrimonio di soggetti diversi dai soci e dai creditori, salvo che sia commesso in danno dello Stato, di altri enti pubblici o delle Comunità europee.</p> <p>Nel caso di società soggette alle disposizioni della parte IV, titolo III, capo II, del testo unico di cui al decreto legislativo 24 febbraio 1998, n. 58, e successive modificazioni, la pena per i fatti previsti al primo comma è da uno a quattro anni e il delitto è procedibile d'ufficio.</p> <p>La pena è da due a sei anni se, nelle ipotesi di cui al terzo comma, il fatto cagiona un grave nocumento ai risparmiatori.</p> <p>Il nocumento si considera grave quando abbia riguardato un numero di risparmiatori superiore allo 0,1 per mille della popolazione risultante dall'ultimo censimento ISTAT ovvero se sia consistito nella distruzione o riduzione del valore di titoli di entità complessiva superiore allo 0,1 per mille del prodotto interno lordo.</p> <p>La punibilità per i fatti previsti dal primo e terzo comma è estesa anche al caso in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi.</p> <p>La punibilità per i fatti previsti dal primo e terzo comma è esclusa se le falsità o le omissioni non alterano in modo sensibile la rappresentazione della situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene. La punibilità è comunque esclusa se le falsità o le omissioni determinano una variazione del risultato economico di esercizio, al lordo delle imposte, non superiore al 5 per cento o una variazione del patrimonio netto non superiore all'1 per cento.</p> <p>In ogni caso il fatto non è punibile se conseguenza di valutazioni estimative che, singolarmente considerate, differiscono in misura non superiore al 10 per cento da quella corretta.</p> <p>Nei casi previsti dai commi settimo e ottavo, ai soggetti di cui al primo comma sono irrogate la sanzione amministrativa da dieci a cento quote e l'interdizione dagli uffici direttivi delle persone giuridiche e delle imprese da sei mesi a tre anni, dall'esercizio dell'ufficio di amministratore,</p>

	sindaco, liquidatore, direttore generale e dirigente preposto alla redazione dei documenti contabili societari, nonché da ogni altro ufficio con potere di rappresentanza della persona giuridica o dell'impresa
173 bis TU 58/98 Falso in prospetto	Chiunque, allo scopo di conseguire per sé o per altri un ingiusto profitto, nei prospetti per la sollecitazione all'investimento o l'ammissione alla quotazione nei mercati regolamentati, ovvero nei documenti da pubblicare in occasione delle offerte pubbliche di acquisto o di scambio, con l'intenzione di ingannare i destinatari del prospetto, espone false informazioni o occulta dati o notizie in modo idoneo ad indurre in errore i suddetti destinatari è punito con la reclusione da uno a cinque anni.
2624. Falsità nelle relazioni o nelle comunicazioni delle società di revisione.	I responsabili della revisione i quali, al fine di conseguire per sé o per altri un ingiusto profitto, nelle relazioni o in altre comunicazioni, con la consapevolezza della falsità e l'intenzione di ingannare i destinatari delle comunicazioni, attestano il falso od occultano informazioni concernenti la situazione economica, patrimoniale o finanziaria della società, ente o soggetto sottoposto a revisione, in modo idoneo ad indurre in errore i destinatari delle comunicazioni sulla predetta situazione, sono puniti, se la condotta non ha loro cagionato un danno patrimoniale, con l'arresto fino a un anno. Se la condotta di cui al primo comma ha cagionato un danno patrimoniale ai destinatari delle comunicazioni, la pena è della reclusione da uno a quattro anni
2625. Impedito controllo.	Gli amministratori che, occultando documenti o con altri idonei artifici, impediscono o comunque ostacolano lo svolgimento delle attività di controllo o di revisione legalmente attribuite ai soci, ad altri organi sociali o alle società di revisione, sono puniti con la sanzione amministrativa pecuniaria fino a 10.329 euro. Se la condotta ha cagionato un danno ai soci, si applica la reclusione fino ad un anno e si procede a querela della persona offesa . La pena è raddoppiata se si tratta di società con titoli quotati in mercati regolamentati italiani o di altri Stati dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi dell'articolo 116 del testo unico di cui al decreto legislativo 24 febbraio 1998, n. 58
2626. Indebita restituzione dei conferimenti.	Gli amministratori che, fuori dei casi di legittima riduzione del capitale sociale, restituiscono, anche simulatamente, i conferimenti ai soci o li liberano dall'obbligo di eseguirli, sono puniti con la reclusione fino ad un anno.

2627. Illegale ripartizione degli utili e delle riserve.	Salvo che il fatto non costituisca più grave reato, gli amministratori che ripartiscono utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva, ovvero che ripartiscono riserve, anche non costituite con utili, che non possono per legge essere distribuite, sono puniti con l'arresto fino ad un anno. La restituzione degli utili o la ricostituzione delle riserve prima del termine previsto per l'approvazione del bilancio estingue il reato
2628. Illecite operazioni sulle azioni o quote sociali o della società controllante.	Gli amministratori che, fuori dei casi consentiti dalla legge, acquistano o sottoscrivono azioni o quote sociali, cagionando una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge, sono puniti con la reclusione fino ad un anno. La stessa pena si applica agli amministratori che, fuori dei casi consentiti dalla legge, acquistano o sottoscrivono azioni o quote emesse dalla società controllante, cagionando una lesione del capitale sociale o delle riserve non distribuibili per legge. Se il capitale sociale o le riserve sono ricostituiti prima del termine previsto per l'approvazione del bilancio relativo all'esercizio in relazione al quale è stata posta in essere la condotta, il reato è estinto
2629. Operazioni in pregiudizio dei creditori.	Gli amministratori che, in violazione delle disposizioni di legge a tutela dei creditori, effettuano riduzioni del capitale sociale o fusioni con altra società o scissioni, cagionando danno ai creditori, sono puniti, a querela della persona offesa, con la reclusione da sei mesi a tre anni. Il risarcimento del danno ai creditori prima del giudizio estingue il reato
2629- bis. Omessa comunicazione del conflitto di interessi	L'amministratore o il componente del consiglio di gestione di una società con titoli quotati in mercati regolamentati italiani o di altro Stato dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi dell'articolo 116 del testo unico di cui al decreto legislativo 24 febbraio 1998, n. 58, e successive modificazioni, ovvero di un soggetto sottoposto a vigilanza ai sensi del testo unico di cui al decreto legislativo 1° settembre 1993, n. 385, del citato testo unico di cui al decreto legislativo n. 58 del 1998, del decreto legislativo 7 settembre 2005, n. 209, o del decreto legislativo 21 aprile 1993, n. 124, che viola gli obblighi previsti dall'articolo 2391, primo comma, è punito con la reclusione da uno a tre anni, se dalla violazione siano derivati danni alla società o a terzi.
2632. Formazione fittizia del capitale.	Gli amministratori e i soci conferenti che, anche in parte, formano od aumentano fittiziamente il capitale sociale mediante attribuzioni di azioni o quote in misura complessivamente superiore all'ammontare del capitale sociale, sottoscrizione reciproca di azioni o quote, sopravvalutazione rilevante dei conferimenti di beni in natura o di crediti ovvero del patrimonio della società nel caso di trasformazione, sono puniti con la reclusione fino ad un anno
2633. Indebita ripartizione dei beni sociali da parte dei liquidatori.	I liquidatori che, ripartendo i beni sociali tra i soci prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessario a soddisfarli, cagionano danno ai creditori, sono puniti, a querela della persona offesa, con la reclusione da sei mesi a tre anni. Il risarcimento del danno ai creditori prima del giudizio estingue il reato
2636. Illecita influenza sull'assemblea	Chiunque, con atti simulati o fraudolenti, determina la maggioranza in assemblea, allo scopo di procurare a sé o ad altri un ingiusto profitto, è punito con la reclusione da sei mesi a tre anni
2637. Aggotaggio.	Chiunque diffonde notizie false, ovvero pone in essere operazioni simulate o altri artifici concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato, ovvero ad incidere in modo significativo sull'affidamento che il pubblico ripone nella stabilità patrimoniale di banche o di gruppi bancari, è punito con la pena della reclusione da uno a cinque anni

<p>2638. Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza.</p>	<p>Gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori di società o enti e gli altri soggetti sottoposti per legge alle autorità pubbliche di vigilanza, o tenuti ad obblighi nei loro confronti, i quali nelle comunicazioni alle predette autorità previste in base alla legge, al fine di ostacolare l'esercizio delle funzioni di vigilanza, espongono fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, sulla situazione economica, patrimoniale o finanziaria dei sottoposti alla vigilanza ovvero, allo stesso fine, occultano con altri mezzi fraudolenti, in tutto o in parte fatti che avrebbero dovuto comunicare, concernenti la situazione medesima, sono puniti con la reclusione da uno a quattro anni. La punibilità è estesa anche al caso in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi.</p> <p>Sono puniti con la stessa pena gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori di società, o enti e gli altri soggetti sottoposti per legge alle autorità pubbliche di vigilanza o tenuti ad obblighi nei loro confronti, i quali, in qualsiasi forma, anche omettendo le comunicazioni dovute alle predette autorità, consapevolmente ne ostacolano le funzioni.</p> <p>La pena è raddoppiata se si tratta di società con titoli quotati in mercati regolamentati italiani o di altri Stati dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi dell'articolo 116 del testo unico di cui al decreto legislativo 24 febbraio 1998, n. 58</p>
--	--

Reati di terrorismo e di eversione dell'ordine democratico

<p>270. Associazioni sovversive.</p>	<p>Chiunque nel territorio dello Stato promuove, costituisce, organizza o dirige associazioni dirette e idonee a sovvertire violentemente gli ordinamenti economici o sociali costituiti nello Stato ovvero a sopprimere violentemente l'ordinamento politico e giuridico dello Stato, è punito con la reclusione da cinque a dieci anni . Chiunque partecipa alle associazioni di cui al primo comma è punito con la reclusione da uno a tre anni. Le pene sono aumentate per coloro che ricostituiscono, anche sotto falso nome o forma simulata, le associazioni di cui al primo comma, delle quali sia stato ordinato lo scioglimento.</p>
<p>270-bis. (Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico).</p>	<p>Chiunque promuove, costituisce, organizza, dirige o finanzia associazioni che si propongono il compimento di atti di violenza con finalità di terrorismo o di eversione dell'ordine democratico è punito con la reclusione da sette a quindici anni. Chiunque partecipa a tali associazioni è punito con la reclusione da cinque a dieci anni. Ai fini della legge penale, la finalità di terrorismo ricorre anche quando gli atti di violenza sono rivolti contro uno Stato estero, un'istituzione o un organismo internazionale. Nei confronti del condannato è sempre obbligatoria la confisca delle cose che servono o furono destinate a commettere il reato e delle cose che ne sono il prezzo, il prodotto, il profitto o che ne costituiscono l'impiego</p>
<p>270-ter. Assistenza agli associati.</p>	<p>Chiunque, fuori dei casi di concorso nel reato o di favoreggiamento, dà rifugio o fornisce vitto, ospitalità, mezzi di trasporto, strumenti di comunicazione a taluna delle persone che partecipano alle associazioni indicate negli articoli 270 e 270-bis è punito con la reclusione fino a quattro anni. La pena è aumentata se l'assistenza è prestata continuativamente. Non è punibile chi commette il fatto in favore di un prossimo congiunto .</p>
<p>270-quater. Arruolamento con finalità di terrorismo anche internazionale</p>	<p>Chiunque, al di fuori dei casi di cui all'articolo 270-bis, arruola una o più persone per il compimento di atti di violenza ovvero di sabotaggio di servizi pubblici essenziali, con finalità di terrorismo, anche se rivolti contro uno Stato estero, un'istituzione o un organismo internazionale, è punito con la reclusione da sette a quindici anni .</p>
<p>270-quinquies. Addestramento ad attività con finalità di terrorismo anche internazionale.</p>	<p>Chiunque, al di fuori dei casi di cui all'articolo 270-bis, addestra o comunque fornisce istruzioni sulla preparazione o sull'uso di materiali esplosivi, di armi da fuoco o di altre armi, di sostanze chimiche o batteriologiche nocive o pericolose, nonché di ogni altra tecnica o metodo per il compimento di atti di violenza ovvero di sabotaggio di servizi pubblici essenziali, con finalità di terrorismo, anche se rivolti contro uno Stato estero, un'istituzione o un organismo internazionale, è punito con la reclusione da cinque a dieci anni. La stessa pena si applica nei confronti della persona addestrata .</p>
<p>270-sexies. Condotte con finalità di terrorismo.</p>	<p>Sono considerate con finalità di terrorismo le condotte che, per la loro natura o contesto, possono arrecare grave danno ad un Paese o ad un'organizzazione internazionale e sono compiute allo scopo di intimidire la popolazione o costringere i poteri pubblici o un'organizzazione internazionale a compiere o astenersi dal compiere un qualsiasi atto o destabilizzare o distruggere le strutture politiche fondamentali, costituzionali, economiche e sociali di un Paese o di un'organizzazione internazionale, nonché le altre condotte definite terroristiche o commesse con finalità di terrorismo da convenzioni o altre norme di diritto internazionale vincolanti per l'Italia.</p>
<p>280. Attentato per finalità terroristiche o di eversione</p>	<p>Chiunque per finalità di terrorismo o di eversione dell'ordine democratico attenta alla vita od alla incolumità di una persona, è punito, nel primo caso, con la reclusione non inferiore ad anni venti e, nel secondo caso, con la reclusione non inferiore ad anni sei. Se dall'attentato alla incolumità di una persona deriva una lesione gravissima, si applica la pena della reclusione non inferiore ad anni diciotto; se ne deriva una lesione grave, si applica la pena della reclusione non inferiore ad anni dodici. Se i fatti previsti nei commi precedenti sono rivolti contro persone che esercitano funzioni giudiziarie o penitenziarie ovvero di sicurezza pubblica nell'esercizio o a</p>

	<p>causa delle loro funzioni, le pene sono aumentate di un terzo.</p> <p>Se dai fatti di cui ai commi precedenti deriva la morte della persona si applicano nel caso di attentato alla vita, l'ergastolo e, nel caso di attentato alla incolumità, la reclusione di anni trenta.</p> <p>Le circostanze attenuanti, diverse da quelle previste dagli articoli 98 e 114, concorrenti con le aggravanti di cui al secondo e al quarto comma, non possono essere ritenute equivalenti o prevalenti rispetto a queste e le diminuzioni di pena si operano sulla quantità di pena risultante dall'aumento conseguente alle predette aggravanti .</p>
280-bis. Atto di terrorismo con ordigni micidiali o esplosivi.	<p>Salvo che il fatto costituisca più grave reato, chiunque per finalità di terrorismo compie qualsiasi atto diretto a danneggiare cose mobili o immobili altrui, mediante l'uso di dispositivi esplosivi o comunque micidiali, è punito con la reclusione da due a cinque anni.</p> <p>Ai fini del presente articolo, per dispositivi esplosivi o comunque micidiali si intendono le armi e le materie ad esse assimilate indicate nell'articolo 585 e idonee a causare importanti danni materiali.</p> <p>Se il fatto è diretto contro la sede della Presidenza della Repubblica, delle Assemblee legislative, della Corte costituzionale, di organi del Governo o comunque di organi previsti dalla Costituzione o da leggi costituzionali, la pena è aumentata fino alla metà.</p> <p>Se dal fatto deriva pericolo per l'incolumità pubblica ovvero un grave danno per l'economia nazionale, si applica la reclusione da cinque a dieci anni.</p> <p>Le circostanze attenuanti, diverse da quelle previste dagli articoli 98 e 114, concorrenti con le aggravanti di cui al terzo e al quarto comma, non possono essere ritenute equivalenti o prevalenti rispetto a queste e le diminuzioni di pena si operano sulla quantità di pena risultante dall'aumento conseguente alle predette aggravanti .</p>
289-bis. Sequestro di persona a scopo di terrorismo o di eversione.	<p>Chiunque, per finalità di terrorismo o di eversione dell'ordine democratico sequestra una persona è punito con la reclusione da venticinque a trenta anni.</p> <p>Se dal sequestro deriva comunque la morte, quale conseguenza non voluta dal reo, della persona sequestrata, il colpevole è punito con la reclusione di anni trenta.</p> <p>Se il colpevole cagiona la morte del sequestrato si applica la pena dell'ergastolo.</p> <p>Il concorrente che, dissociandosi dagli altri, si adopera in modo che il soggetto passivo riacquisti la libertà è punito con la reclusione da due a otto anni; se il soggetto passivo muore, in conseguenza del sequestro, dopo la liberazione, la pena è della reclusione da otto a diciotto anni .</p> <p>Quando ricorre una circostanza attenuante, alla pena prevista dal secondo comma è sostituita la reclusione da venti a ventiquattro anni; alla pena prevista dal terzo comma è sostituita la reclusione da ventiquattro a trenta anni. Se concorrono più circostanze attenuanti, la pena da applicare per effetto delle diminuzioni non può essere inferiore a dieci anni, nell'ipotesi prevista dal secondo comma, ed a quindici anni, nell'ipotesi prevista dal terzo comma .</p>
414. Istigazione a delinquere.	<p>Chiunque pubblicamente istiga a commettere uno o più reati è punito, per il solo fatto dell'istigazione:</p> <ol style="list-style-type: none"> 1. con la reclusione da uno a cinque anni, se trattasi di istigazione a commettere delitti ; 2. con la reclusione fino a un anno, ovvero con la multa fino a euro 206 , se trattasi di istigazione a commettere contravvenzioni . <p>Se si tratta di istigazione a commettere uno o più delitti e una o più contravvenzioni, si applica la pena stabilita nel n. 1.</p> <p>Alla pena stabilita del n. 1 soggiace anche chi pubblicamente fa l'apologia di uno o più delitti .</p> <p>Fuori dei casi di cui all'articolo 302, se l'istigazione o l'apologia di cui ai commi precedenti riguarda delitti di terrorismo o crimini contro l'umanità la pena è aumentata della metà .</p>

<p>Convenzione per la repressione del finanziamento del terrorismo</p>	<p>Commet une infraction au sens de la presente convention tout personne qui, par quelque moyen que ce soit, directement o indirectement, illicitement et deliberelement, fournit ou reunit des fonds dans l'intention de les voir utilises ou en sachant qu'ils seront utilises, en tout ou partie, en veu de commettre:</p> <p>a. Un acte qui constitue une infraction au regard et selon la definition de l'undes traites enumeres en annexe;</p> <p>b. Tout autre acte destine a tuer ou blesser grievement un civil, ou toute autre personne qui ne participe pas directment aux hostilites dans une situation de conflict armè, lorsque, par sa nature ou son contexte, cet acte vise a intimider une population ou a contraindre un gouvernement ou une organisatin internationale a accomplir ou a s'abstenir d'accomplir un acte quelconque.</p>
---	---

Reati contro la persona

<p>583-bis. Pratiche di mutilazione degli organi genitali femminili.</p>	<p>Chiunque, in assenza di esigenze terapeutiche, cagiona una mutilazione degli organi genitali femminili è punito con la reclusione da quattro a dodici anni. Ai fini del presente articolo, si intendono come pratiche di mutilazione degli organi genitali femminili la clitoridectomia, l'escissione e l'infibulazione e qualsiasi altra pratica che cagioni effetti dello stesso tipo.</p> <p>Chiunque, in assenza di esigenze terapeutiche, provoca, al fine di menomare le funzioni sessuali, lesioni agli organi genitali femminili diverse da quelle indicate al primo comma, da cui derivi una malattia nel corpo o nella mente, è punito con la reclusione da tre a sette anni. La pena è diminuita fino a due terzi se la lesione è di lieve entità.</p> <p>La pena è aumentata di un terzo quando le pratiche di cui al primo e al secondo comma sono commesse a danno di un minore ovvero se il fatto è commesso per fini di lucro.</p> <p>Le disposizioni del presente articolo si applicano altresì quando il fatto è commesso all'estero da cittadino italiano o da straniero residente in Italia, ovvero in danno di cittadino italiano o di straniero residente in Italia. In tal caso, il colpevole è punito a richiesta del Ministro della giustizia</p>
<p>600. Riduzione o mantenimento in schiavitù o in servitù</p>	<p>Chiunque esercita su una persona poteri corrispondenti a quelli dle diritto di proprietà ovvero chiunque riduce o mantiene una persona in uno stato di soggezione continuativa, costringendola a prestazioni lavorative o sessuali ovvero all'accattonaggio o comunque a prestazioni che ne comportino lo sfruttamento è punito con la reclusione da otto a venti anni.</p> <p>La riduzione o il mantenimento nello stato di soggezione ha luogo quando la condotta è attuata mediante violenza, minaccia, inganno, abuso di autorità o approfittamento di una situazione di inferiorità fisica o psichica o di una situazione di necessità o mediante la promessa o la dazione di somme di denaro o altri vantaggi a chi ha autorità sulla persona.</p> <p>La pena è aumentata da un terzo alla metà se i fattidi cui al primocomma sono commessi in danno di minore degli anni 18° sono diretti allo sfruttamento della prostituzione o al fine di sottoporre la persona offesa al prelievo di organi.</p>
<p>600-bis. Prostituzione minorile.</p>	<p>Chiunque induce alla prostituzione una persona di età inferiore agli anni diciotto ovvero ne favorisce o sfrutta la prostituzione è punito con la reclusione da sei a dodici anni e con la multa da lire trenta milioni a lire trecento milioni.</p> <p>Salvo che il fatto costituisca più grave reato, chiunque compie atti sessuali con un minore di età compresa fra i quattordici ed i sedici anni, in cambio di denaro o di altra utilità economica, è punito con la reclusione da sei mesi a tre anni o con la multa non inferiore a lire dieci milioni. La pena è ridotta di un terzo se colui che commette il fatto è persona minore degli anni diciotto.</p>
<p>600-ter. Pornografia minorile.</p>	<p>Chiunque sfrutta minori degli anni diciotto al fine di realizzare esibizioni pornografiche o di produrre materiale pornografico è punito con la reclusione da sei a dodici anni e con la multa da lire cinquanta milioni a lire cinquecento milioni.</p> <p>Alla stessa pena soggiace chi fa commercio del materiale pornografico di cui al primo comma.</p> <p>Chiunque, al di fuori delle ipotesi di cui al primo e al secondo comma, con</p>

	<p>qualsiasi mezzo, anche per via telematica, distribuisce, divulga o pubblicizza il materiale pornografico di cui al primo comma, ovvero distribuisce o divulga notizie o informazioni finalizzate all'adescamento o allo sfruttamento sessuale di minori degli anni diciotto, è punito con la reclusione da uno a cinque anni e con la multa da lire cinque milioni a lire cento milioni.</p> <p>Chiunque, al di fuori delle ipotesi di cui ai commi primo, secondo e terzo, consapevolmente cede ad altri, anche a titolo gratuito, materiale pornografico prodotto mediante lo sfruttamento sessuale dei minori degli anni diciotto, è punito con la reclusione fino a tre anni o con la multa da lire tre milioni a lire dieci milioni</p>
600-quater. Detenzione di materiale pornografico.	Chiunque, al di fuori delle ipotesi previste nell'articolo 600-ter, consapevolmente si procura o dispone di materiale pornografico prodotto mediante lo sfruttamento sessuale dei minori degli anni diciotto è punito con la reclusione fino a tre anni o con la multa non inferiore a lire tre milioni
600-quater 1. Pornografia virtuale	Le disposizioni di cui agli articoli 600 ter e 600 quater si applicano anche quando il materiale pronografico rappresenta immagini virtuali realizzate utilizzando immagini di minori degli anni diciotto o parti di esse, ma la pena è diminuita di un terzo. Per immagini virtuali si intendono immagini realizzati con tecniche di elaborazione grafica non associate in tutto o in parte a situazioni reali la cui qualità di rappresentazione fa apparire come vere situazioni non reali.
600-quinquies. Iniziative turistiche volte allo sfruttamento della prostituzione minorile.	Chiunque organizza o propaganda viaggi finalizzati alla fruizione di attività di prostituzione a danno di minori o comunque comprendenti tale attività è punito con la reclusione da sei a dodici anni e con la multa da lire trenta milioni a lire trecento milioni
601. Tratta di persone.	Chiunque commette tratta di persona che si trova nelle condizioni di cui all'articolo 600 ovvero, al fine di commettere i delitti di cui al primo comma del medesimo articolo, la induce mediante inganno o la costringe mediante violenza, minaccia, abuso di autorità o approfittamento di una situazione di inferiorità fisica o psichica o di una situazione di necessità, o mediante promessa o dazione di somme di denaro o di altri vantaggi alla persona che su di essa ha autorità, a fare ingresso o a soggiornare o a uscire dal territorio dello Stato o a trasferirsi al suo interno, è punito con la reclusione da otto a venti anni. La pena è aumentata da un terzo alla metà se i delitti di cui al presente articolo sono commessi in danno di minore degli anni diciotto o sono diretti allo sfruttamento della prostituzione o al fine di sottoporre la persona offesa al prelievo di organi
602. Acquisto e alienazione di schiavi.	Chiunque, fuori dei casi indicati nell'articolo 601, acquista o aliena o cede una persona che si trova in una delle condizioni di cui all'articolo 600 è punito con la reclusione da otto a venti anni. La pena è aumentata da un terzo alla metà se la persona offesa è minore degli anni diciotto ovvero se i fatti di cui al primo comma sono diretti allo sfruttamento della prostituzione o al fine di sottoporre la persona offesa al prelievo di organi

Reati relativi alla manipolazione del mercato

TU 58/98 184. Abuso di informazioni privilegiate.	<p>1. È punito con la reclusione da uno a sei anni e con la multa da euro ventimila a euro tre milioni chiunque, essendo in possesso di informazioni privilegiate in ragione della sua qualità di membro di organi di amministrazione, direzione o controllo dell'emittente, della partecipazione al capitale dell'emittente, ovvero dell'esercizio di un'attività lavorativa, di una professione o di una funzione, anche pubblica, o di un ufficio (101/dd):</p> <p>a) acquista, vende o compie altre operazioni, direttamente o indirettamente, per conto proprio o per conto di terzi, su strumenti finanziari utilizzando le informazioni medesime;</p> <p>b) comunica tali informazioni ad altri, al di fuori del normale esercizio del lavoro, della professione, della funzione o dell'ufficio;</p> <p>c) raccomanda o induce altri, sulla base di esse, al compimento di taluna delle operazioni indicate nella lettera a).</p> <p>2. La stessa pena di cui al comma 1 si applica a chiunque essendo in possesso di informazioni privilegiate a motivo della preparazione o</p>
--	--

	<p>esecuzione di attività delittuose compie taluna delle azioni di cui al medesimo comma 1.</p> <p>3. Il giudice può aumentare la multa fino al triplo o fino al maggiore importo di dieci volte il prodotto o il profitto conseguito dal reato quando, per la rilevante offensività del fatto, per le qualità personali del colpevole o per l'entità del prodotto o del profitto conseguito dal reato, essa appare inadeguata anche se applicata nel massimo.</p> <p>4. Ai fini del presente articolo per strumenti finanziari si intendono anche gli strumenti finanziari di cui all'articolo 1, comma 2, il cui valore dipende da uno strumento finanziario di cui all'articolo 180, comma 1, lettera a)</p>
<p>TU 58/98 185. Manipolazione del mercato</p>	<p>1. Chiunque diffonde notizie false o pone in essere operazioni simulate o altri artifici concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari, è punito con la reclusione da uno a sei anni e con la multa da euro ventimila a euro cinque milioni.</p> <p>2. Il giudice può aumentare la multa fino al triplo o fino al maggiore importo di dieci volte il prodotto o il profitto conseguito dal reato quando, per la rilevante offensività del fatto, per le qualità personali del colpevole o per l'entità del prodotto o del profitto conseguito dal reato, essa appare inadeguata anche se applicata nel massimo.</p>

Reati ex lege 146/06

<p>416 cp Associazione per delinquere</p>	<p>Quando tre o più persone si associano allo scopo di commettere più delitti, coloro che promuovono o costituiscono od organizzano l'associazione sono puniti, per ciò solo, con la reclusione da tre a sette anni.</p> <p>Per il solo fatto di partecipare all'associazione, la pena è della reclusione da uno a cinque anni.</p> <p>I capi soggiacciono alla stessa pena stabilita per i promotori.</p> <p>Se gli associati scendono in armi le campagne o le pubbliche vie si applica la reclusione da cinque a quindici anni.</p> <p>La pena è aumentata se il numero degli associati è di dieci o più.</p> <p>Se l'associazione è diretta a commettere taluno dei delitti di cui agli articoli 600, 601 e 602, si applica la reclusione da cinque a quindici anni nei casi previsti dal primo comma e da quattro a nove anni nei casi previsti dal secondo comma.</p>
<p>416-bis. Associazione di tipo mafioso</p>	<p>Chiunque fa parte di un'associazione di tipo mafioso formata da tre o più persone, è punito con la reclusione da cinque a dieci anni.</p> <p>Coloro che promuovono, dirigono o organizzano l'associazione sono puniti, per ciò solo, con la reclusione da sette a dodici anni.</p> <p>L'associazione è di tipo mafioso quando coloro che ne fanno parte si avvalgano della forza di intimidazione del vincolo associativo e della condizione di assoggettamento e di omertà che ne deriva per commettere delitti, per acquisire in modo diretto o indiretto la gestione o comunque il controllo di attività economiche, di concessioni, di autorizzazioni, appalti e servizi pubblici o per realizzare profitti o vantaggi ingiusti per sé o per altri, ovvero al fine di impedire od ostacolare il libero esercizio del voto o di procurare voti a sé o ad altri in occasione di consultazioni elettorali.</p> <p>Se l'associazione è armata si applica la pena della reclusione da sette a quindici anni nei casi previsti dal primo comma e da dieci a ventiquattro anni nei casi previsti dal secondo comma.</p> <p>L'associazione si considera armata quando i partecipanti hanno la disponibilità, per il conseguimento della finalità dell'associazione, di armi o materie esplosive, anche se occultate o tenute in luogo di deposito.</p> <p>Se le attività economiche di cui gli associati intendono assumere o mantenere il controllo sono finanziate in tutto o in parte con il prezzo, il prodotto, o il profitto di delitti, le pene stabilite nei commi precedenti sono aumentate da un terzo alla metà.</p> <p>Nei confronti del condannato è sempre obbligatoria la confisca delle cose che servono o furono destinate a commettere il reato e delle cose che ne sono il prezzo, il prodotto, il profitto o che ne costituiscono l'impiego.</p>

	Le disposizioni del presente articolo si applicano anche alla camorra e alle altre associazioni, comunque localmente denominate, che valendosi della forza intimidatrice del vincolo associativo perseguono scopi corrispondenti a quelli delle associazioni di tipo mafioso.
291 quater TU 43/73 Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri.	<p>1. Quando tre o più persone si associano allo scopo di commettere più delitti tra quelli previsti dall'articolo 291-bis, coloro che promuovono, costituiscono, dirigono, organizzano o finanziano l'associazione sono puniti, per ciò solo, con la reclusione da tre a otto anni.</p> <p>2. Chi partecipa all'associazione è punito con la reclusione da un anno a sei anni.</p> <p>3. La pena è aumentata se il numero degli associati è di dieci o più.</p> <p>4. Se l'associazione è armata ovvero se ricorrono le circostanze previste dalle lettere d) od e) del comma 2 dell'articolo 291-ter, si applica la pena della reclusione da cinque a quindici anni nei casi previsti dal comma 1 del presente articolo, e da quattro a dieci anni nei casi previsti dal comma 2. L'associazione si considera armata quando i partecipanti hanno la disponibilità, per il conseguimento delle finalità dell'associazione, di armi o materie esplodenti, anche se occultate o tenute in luogo di deposito.</p> <p>5. Le pene previste dagli articoli 291-bis, 291-ter e dal presente articolo sono diminuite da un terzo alla metà nei confronti dell'imputato che, dissociandosi dagli altri, si adopera per evitare che l'attività delittuosa sia portata ad ulteriori conseguenze anche aiutando concretamente l'autorità di polizia o l'autorità giudiziaria nella raccolta di elementi decisivi per la ricostruzione dei fatti e per l'individuazione o la cattura degli autori del reato o per la individuazione di risorse rilevanti per la commissione dei delitti.</p>
74 TU 309/90 Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope	<p>1. Quando tre o più persone si associano allo scopo di commettere più delitti tra quelli previsti dall'articolo 73, chi promuove, costituisce, dirige, organizza o finanzia l'associazione è punito per ciò solo con la reclusione non inferiore a venti anni.</p> <p>2. Chi partecipa all'associazione è punito con la reclusione non inferiore a dieci anni.</p> <p>3. La pena è aumentata se il numero degli associati è di dieci o più o se tra i partecipanti vi sono persone dedite all'uso di sostanze stupefacenti o psicotrope.</p> <p>4. Se l'associazione è armata la pena, nei casi indicati dai commi 1 e 3, non può essere inferiore a ventiquattro anni di reclusione e, nel caso previsto dal comma 2, a dodici anni di reclusione. L'associazione si considera armata quando i partecipanti hanno la disponibilità di armi o materie esplodenti, anche se occultate o tenute in luogo di deposito.</p> <p>5. La pena è aumentata se ricorre la circostanza di cui alla lettera e) del comma 1 dell'articolo 80.</p> <p>6. Se l'associazione è costituita per commettere i fatti descritti dal comma 5 dell'articolo 73, si applicano il primo e il secondo comma dell'articolo 416 del codice penale.</p> <p>7. Le pene previste dai commi da 1 a 6 sono diminuite dalla metà a due terzi per chi si sia efficacemente adoperato per assicurare le prove del reato o per sottrarre all'associazione risorse decisive per la commissione dei delitti.</p> <p>8. Quando in leggi e decreti è richiamato il reato previsto dall'articolo 75 della legge 22 dicembre 1975, n. 685, abrogato dall'articolo 38, comma 1, della legge 26 giugno 1990, n. 162, il richiamo si intende riferito al presente articolo.</p>
377 bis Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria.	Salvo che il fatto costituisca più grave reato, chiunque, con violenza o minaccia, o con offerta o promessa di denaro o di altra utilità, induce a non rendere dichiarazioni o a rendere dichiarazioni mendaci la persona chiamata a rendere davanti alla autorità giudiziaria dichiarazioni utilizzabili in un procedimento penale, quando questa ha la facoltà di non rispondere, è punito con la reclusione da due a sei anni
378 Favoreggiamento personale	<p>Chiunque, dopo che fu commesso un delitto per il quale la legge stabilisce la pena di morte o l'ergastolo o la reclusione, e fuori dei casi di concorso nel medesimo, aiuta taluno a eludere le investigazioni dell'autorità, o a sottrarsi alle ricerche di questa, è punito con la reclusione fino a quattro anni.</p> <p>Quando il delitto commesso è quello previsto dall'art. 416-bis, si applica, in ogni caso, la pena della reclusione non inferiore a due anni.</p> <p>Se si tratta di delitti per i quali la legge stabilisce una pena diversa, ovvero di contravvenzioni, la pena è della multa fino a lire un milione</p> <p>Le disposizioni di questo articolo si applicano anche quando la persona aiutata non è imputabile o risulta che non ha commesso il delitto</p>

Reati di omicidio colposo e lesioni gravi o gravissime commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro

<p>589 Omicidio colposo</p>	<p>Chiunque cagiona per colpa la morte di una persona è punito con la reclusione da sei mesi a cinque anni. Se il fatto è commesso con violazione delle norme sulla disciplina della circolazione stradale o di quelle per la prevenzione degli infortuni sul lavoro la pena è della reclusione da due a cinque anni. Nel caso di morte di più persone, ovvero di morte di una o più persone e di lesioni di una o più persone, si applica la pena che dovrebbe infliggersi per la più grave delle violazioni commesse aumentata fino al triplo, ma la pena non può superare gli anni dodici</p>
<p>590 Lesioni colpose (3. comma)</p>	<p>Chiunque cagiona ad altri per colpa una lesione personale è punito con la reclusione fino a tre mesi o con la multa fino a euro 309. Se la lesione è grave la pena è della reclusione da uno a sei mesi o della multa da euro 123 a euro 619, se è gravissima, della reclusione da tre mesi a due anni o della multa da euro 309 a euro 1.239. Se i fatti di cui al secondo comma sono commessi con violazione delle norme sulla disciplina della circolazione stradale o di quelle per la prevenzione degli infortuni sul lavoro la pena per le lesioni gravi è della reclusione da tre mesi a un anno o della multa da euro 500 a euro 2.000 e la pena per le lesioni gravissime è della reclusione da uno a tre anni. Nel caso di lesioni di più persone si applica la pena che dovrebbe infliggersi per la più grave delle violazioni commesse, aumentata fino al triplo; ma la pena della reclusione non può superare gli anni cinque. Il delitto è punibile a querela della persona offesa, salvo nei casi previsti nel primo e secondo capoverso, limitatamente ai fatti commessi con violazione delle norme per la prevenzione degli infortuni sul lavoro o relative all'igiene del lavoro o che abbiano determinato una malattia professionale.</p>

Reati di ricettazione, riciclaggio e impiego di denaro, beni e altre utilità di provenienza illecita

<p>648 Ricettazione</p>	<p>Fuori dei casi di concorso nel reato chi, al fine di procurare a sé o ad altri un profitto, acquista, riceve od occulta denaro o cose provenienti da un qualsiasi delitto, o comunque si intromette nel farle acquistare, ricevere od occultare, è punito con la reclusione da due ad otto anni e con la multa da euro 516 a euro 10.329. La pena è della reclusione sino a sei anni e della multa sino a euro 516, se il fatto è di particolare tenuità. Le disposizioni di questo articolo si applicano anche quando l'autore del delitto da cui il denaro o le cose provengono non è imputabile o non è punibile ovvero quando manchi una condizione di procedibilità riferita a tale delitto.</p>
<p>648 bis Riciclaggio</p>	<p>Fuori dei casi di concorso nel reato, chiunque sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto non colposo, ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa, è punito con la reclusione da quattro a dodici anni e con la multa da lire due milioni a lire trenta milioni. La pena è aumentata quando il fatto è commesso nell'esercizio di un'attività professionale. La pena è diminuita se il denaro, i beni o le altre utilità provengono da delitto per il quale è stabilita la pena della reclusione inferiore nel massimo a cinque anni. Si applica l'ultimo comma dell'articolo 648.</p>
<p>648 ter Impiego di denaro, beni o utilità di provenienza illecita</p>	<p>Chiunque, fuori dei casi di concorso nel reato e dei casi previsti dagli articoli 648 e 648-bis, impiega in attività economiche o finanziarie denaro, beni o altre utilità provenienti da delitto, è punito con la reclusione da quattro a dodici anni e con la multa da lire due milioni a lire trenta milioni.</p>

	<p>La pena è aumentata quando il fatto è commesso nell'esercizio di un'attività professionale.</p> <p>La pena è diminuita nell'ipotesi di cui al secondo comma dell'articolo 648. Si applica l'ultimo comma dell'articolo 648 .</p>
--	---

Reati informatici

<p>615-ter. Accesso abusivo ad un sistema informatico o telematico.</p>	<p>Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.</p> <p>La pena è della reclusione da uno a cinque anni:</p> <p>1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;</p> <p>2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;</p> <p>3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.</p> <p>Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.</p> <p>Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.</p>
<p>615-quater. Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici.</p>	<p>Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a euro 5.164.</p> <p>La pena è della reclusione da uno a due anni e della multa da euro 5.164 a euro 10.329 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617-quater .</p>
<p>615 quinquies Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico</p>	<p>Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329</p>
<p>617-quater. Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche.</p>	<p>Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni.</p> <p>Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma.</p> <p>I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa.</p> <p>Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso:</p> <p>1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;</p> <p>2) da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;</p> <p>3) da chi esercita anche abusivamente la professione di investigatore</p>

	privato
617-quinquies. Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche.	Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni. La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617-quater
635 –bis Danneggiamento di informazioni, dati e programmi informatici	Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni e si procede d'ufficio
635 –ter Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità	Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni. Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata
635 –quater Danneggiamento di sistemi informatici o telematici	Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata
635-quinquies. Danneggiamento di sistemi informatici o telematici di pubblica utilità.	Se il fatto di cui all'articolo 635-quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni. Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata
640-quinquies. Frode informatica del soggetto che presta servizi di certificazione di firma elettronica.	Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, è punito con la reclusione fino a tre anni e con la multa da 51 a 1.032 euro
491 –bis Documenti informatici	Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private

Allegato 2 “Composizione del Consiglio di Amministrazione”

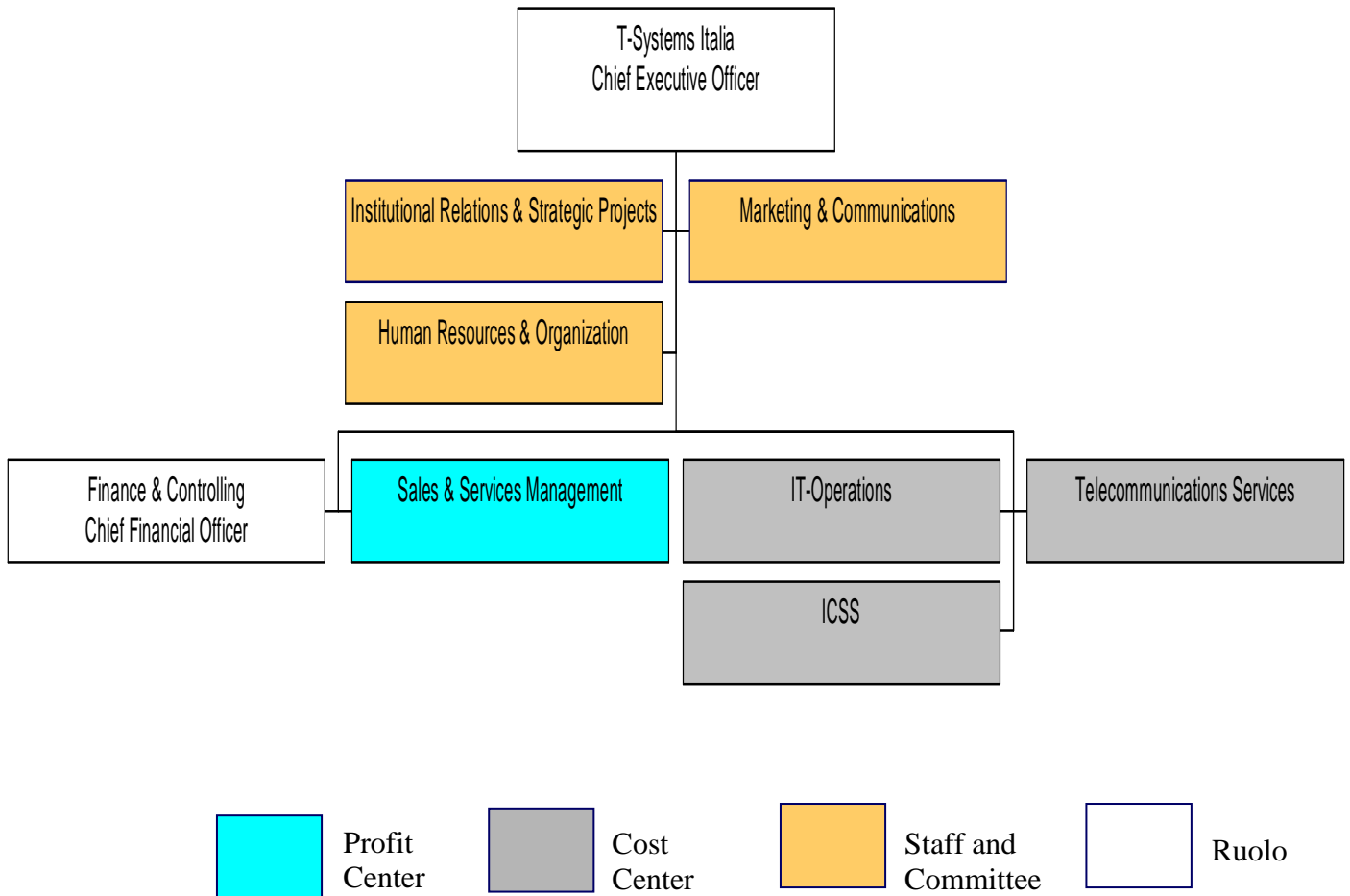
Il Consiglio di Amministrazione di T-Systems Italia s.p.a. alla data del 19 marzo 2008 risulta così composto:

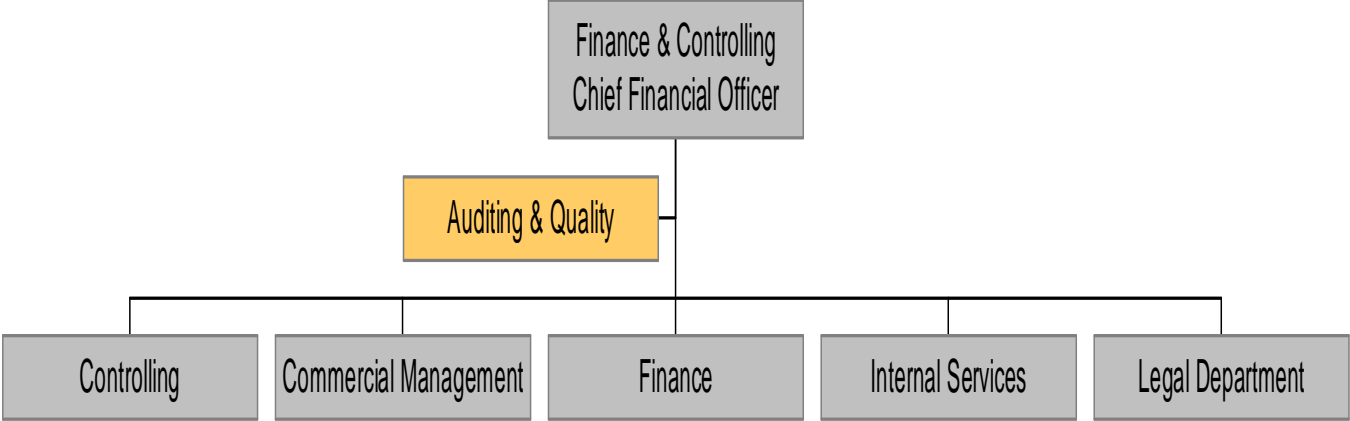
Gunther Horst Fenk	Presidente
Valentino Bravi	Amministratore Delegato
Alexander Hauser	Consigliere
Jeannine Pilloud	Consigliere
Fausto Plebani	Consigliere
Jurgen Hernichel	Consigliere

Il Collegio Sindacale di T-Systems Italia s.p.a. alla data del 19 marzo 2008 risulta così composto:

Francesco Montini	Presidente
Giampietro Sala	Sindaco Effettivo
Giuliano Trivellin	Sindaco Effettivo
Franco Corniati	Sindaco Supplente
Alberto Matteazzi	Sindaco Supplente

Allegato 3 “Organigramma Funzionale”





Allegato 4 “Composizione Advisory Board”

L'Advisory Board di T-Systems Italia s.p.a. alla data del 19 marzo 2008 risulta così composto:

Prof. Giancarlo Elia Valori	Presidente
Prof. Antonio Baldassarre	Membro Effettivo
Dr. Ettore Bernabei	Membro Effettivo
Prof. Pellegrino Capaldo	Membro Effettivo
Prof. Paolo Savona	Membro Effettivo
Valentino Bravi	Membro Effettivo
Fausto Plebani	Membro Effettivo
Giancarlo Maria Albini	Membro Effettivo

Allegato 5 “Sistema di Gestione della Salute e della Sicurezza sul Lavoro”

T-Systems Italia S.p.A
SGSL
Sistema di Gestione della Salute e della Sicurezza sul Lavoro

INTRODUZIONE

Il presente documento descrive il Sistema di Gestione della Salute e della Sicurezza sul Lavoro (d'ora in avanti Sistema) di T-Systems Italia spa.

Il Sistema è adottato ai sensi dell'art. 30 del d.lgs. 81/08 in materia di tutela della salute e della sicurezza nei luoghi di lavoro ed è, quindi, volto a garantire l'adempimento di tutti gli obblighi giuridici relativi:

- a) al rispetto degli standard tecnico-strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;
- b) alle attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;
- c) alle attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza;
- d) alle attività di sorveglianza sanitaria;
- e) alle attività di informazione e formazione dei lavoratori;
- f) alle attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;
- g) alla acquisizione di documentazioni e certificazioni obbligatorie di legge;
- h) alle periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate.

Il Sistema prevede:

- idonee modalità di registrazione dell'effettuazione delle attività;
- un'articolazione di funzioni che assicuri le competenze tecniche e i poteri necessari per la verifica, valutazione, gestione e controllo del rischio;
- un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello;
- idonee modalità di controllo sull'attuazione del modello e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate.

Ai sensi dell'art. 30 comma 5 del d.lgs. 81/08 per la redazione del Sistema si è seguito il modello fornito dalle Linee Guida Uni-Inail (versione ottobre 2003).

Il presente documento segue quindi l'articolazione in capitoli proposta dalle suddette Linee Guida.

1. SCOPO E CAMPO DI APPLICAZIONE DEL SGSL

a. Scopo del SGSL

Ai sensi delle Linee Guida Uni-Inail, lo scopo del Sistema è quello di:

- ridurre progressivamente i costi complessivi della SSL, compresi quelli derivanti da incidenti, infortuni e malattie correlate al lavoro minimizzando i rischi cui possono essere esposti i dipendenti o i terzi (clienti, fornitori, visitatori etc.);
- aumentare la propria efficienza e le proprie prestazioni;
- contribuire a migliorare i livelli di salute e sicurezza sul lavoro;
- migliorare la propria immagine interna ed esterna.

Fermo restante il rispetto delle norme di legge, il SGSL che T-Systems adotta:

- prevede il monitoraggio effettuato preferibilmente con personale interno;
- non è soggetto a certificazione da parte terza;
- consente l'adattamento all'evoluzione di leggi, regolamenti e norme di buona tecnica;
- coinvolge i lavoratori e i loro rappresentanti nel sistema di gestione.

Il SGSL è parte del modello organizzativo adottato da T-Systems ai sensi del d.lgs. 231/01 ed è volto, tra l'altro, a ridurre il rischio di responsabilità amministrativa di T-Systems per i reati di omicidio colposo e lesioni colpose gravi o gravissime per la mancata adozione delle misure a protezione della salute e sicurezza sul lavoro.

b. Campo di applicazione del SGSL

Il SGSL si applica alle attività svolte dall'azienda in tutti i suoi siti e, dove rileva, presso i clienti.

2. TERMINI E DEFINIZIONI

I termini adottati dal presente documento sono quelli contenuti nella normativa di riferimento e vanno quindi intesi secondo le definizioni ivi riportate che qui si riproducono almeno in parte per agevolare la consultazione del documento.

- **Appaltatore:** è il soggetto che si obbliga nei confronti del committente a fornire un'opera e/o una prestazione con mezzi propri.
 - **ASPP:** Addetti al Servizio di Prevenzione e Protezione.
 - **Attrezzatura di lavoro:** qualsiasi macchina, apparecchio, utensile od impianto destinato ad essere usato durante il lavoro. (D.Lgs. 81/08, art. 69)
 - **Datore di lavoro (DdL):** il soggetto titolare del rapporto di lavoro con il lavoratore o, comunque, il soggetto che, secondo il tipo e l'organizzazione dell'impresa, ha la responsabilità dell'impresa stessa ovvero dell'unità produttiva, quale definita ai sensi della lettera i), in quanto titolare dei poteri decisionali e di spesa. (D.Lgs. 81/08, art. 2). Nel caso di T-Systems l'Amministratore Delegato.
 - **Dirigente:** dipendente che ricopre un ruolo caratterizzato da elevato grado di professionalità, autonomia e potere decisionale ed esplica le sue funzioni al fine di promuovere, coordinare e gestire la realizzazione degli obiettivi dell'impresa.
 - **DPI:** Dispositivi di Protezione Individuale.
 - **Fabbricante:** soggetto che produce e immette sul mercato o in servizio macchine, apparecchiature, impianti, dispositivi (DPR 459/96). Il fabbricante può essere sia interno che esterno all'organizzazione.
 - **Incidente:** evento dovuto a causa fortuita che ha la potenzialità di condurre ad un infortunio o di provocare danni alle cose.
 - **Infortunio:** evento dovuto a causa fortuita che produca lesioni corporali obiettivamente riscontrabili, in occasione di lavoro.
 - **Lavoratore:** persona che presta il proprio lavoro alle dipendenze di un datore di lavoro, esclusi gli addetti ai servizi domestici e familiari, con rapporto di lavoro subordinato anche speciale. Sono equiparati i soci lavoratori di cooperative o di società, anche di fatto, che prestano la loro attività per conto delle società e degli enti stessi, e gli utenti dei servizi di orientamento o di formazione scolastica, universitaria e professionale avviati presso datori di lavoro per agevolare o per perfezionare le loro scelte professionali. Sono altresì equiparati gli allievi degli istituti di istruzione ed universitari e i partecipanti a corsi di formazione professionale nei quali si faccia uso di laboratori, macchine, apparecchi ed attrezzature di lavoro in genere, agenti chimici, fisici e biologici. (D.Lgs. 81/08, art. 2)
 - **Luogo di lavoro:** i luoghi destinati a contenere posti di lavoro, ubicati all'interno dell'azienda ovvero dell'unità produttiva, nonché ogni altro luogo nell'area della medesima azienda ovvero unità produttiva comunque accessibile per il lavoro. (D.Lgs. 81/08, art. 62)
 - **Malattia professionale:** evento morboso contratto a causa e nell'esercizio delle lavorazioni svolte.
 - **Medico competente (MC):** medico in possesso di uno dei seguenti titoli:
 - a) specializzazione in medicina del lavoro o in medicina preventiva dei lavoratori e psicotecnica;
 - b) docenza in medicina del lavoro o in medicina preventiva dei lavoratori e psicotecnica o in tossicologia industriale o in igiene industriale o in fisiologia e igiene del lavoro o in clinica del lavoro;
 - c) autorizzazione di cui all'articolo 55 del decreto legislativo 15 agosto 1991, n. 277;
 - d) specializzazione in igiene e medicina preventiva o in medicina legale.
 - **Non conformità (n.c.):** difformità dagli standard adottati o mancato rispetto dei requisiti legali, dei regolamenti, delle pratiche, delle procedure, delle istruzioni operative, dello schema di sistema di gestione adottato.
 - **Obiettivi:** risultati, in termini di prestazioni di SSL, che una organizzazione stabilisce di raggiungere.
 - **OdV:** Organismo di Vigilanza ai sensi del d.lgs. 231/01
 - **Pericolo:** la proprietà intrinseca di un agente, una condizione o una situazione, di poter produrre effetti nocivi.
 - **Posto di lavoro:** postazioni, fisse o variabili, in cui il lavoratore espleta la sua mansione.
 - **Preposto:** soggetto che ha la responsabilità della vigilanza e del controllo dell'operato di altri lavoratori.
 - **Rappresentante dei lavoratori per la sicurezza (RLS):** persona, ovvero persone, eletta o designata per rappresentare i lavoratori per quanto concerne gli aspetti della salute e della sicurezza durante il lavoro, di seguito denominato rappresentante per la sicurezza. (D.Lgs. 81/08, art. 2)
 - **Requisiti legali:** norme di legge e/o regolamenti di livello comunitario, statale, locale, ed ogni impegno assunto volontariamente applicabile all'organizzazione in materia di SSL.
 - **Responsabile del servizio di prevenzione e protezione (RSPP):** persona in possesso delle capacità e dei requisiti professionali di cui all'articolo 32 designata dal datore di lavoro, a cui risponde, per coordinare il servizio di prevenzione e protezione dai rischi (D.Lgs. 81/08, art. 2)
 - **Responsabile del SGSL (RSGSL):** soggetto incaricato dall'Amministratore Delegato, dotato di adeguata capacità ed autorità all'interno dell'azienda, a cui è affidato in tutto o in parte il compito, indipendentemente da ulteriori responsabilità aziendali, di coordinare e verificare che il SGSL sia realizzato in conformità alle Linee Guida UNI-INAIL. (Linee Guida UNI-INAIL)
 - **Rischio:** la probabilità che si raggiunga il potenziale nocivo nelle condizioni di utilizzazione o esposizione.
 - **Servizio di prevenzione e protezione dai rischi (SPP):** insieme delle persone, sistemi e mezzi esterni o interni all'azienda finalizzati all'attività di prevenzione e protezione dai rischi professionali nell'azienda, ovvero unità produttiva. (D.Lgs. 81/08, art. 2)
 - **SGSL:** Sistema di Gestione della Salute e Sicurezza sul Lavoro.
 - **SSL:** Sicurezza e Salute dei Lavoratori.
 - **Terzi:** soggetti diversi dal datore di lavoro, dai dirigenti, dai preposti e dai lavoratori, che possono, a qualsiasi titolo, trovarsi all'interno dei luoghi di lavoro o che possono essere influenzati o influenzare le attività lavorative e/o le condizioni di prevenzione.
 - **Unità produttiva:** stabilimento o struttura finalizzata alla produzione di beni o servizi, dotata di autonomia finanziaria e tecnico-funzionale. (D.Lgs. 81/08, art. 2)
 - **Valutazione del rischio (VDR):** valutazione globale della probabilità e della gravità di possibili lesioni o danni alla salute in una situazione pericolosa per scegliere le adeguate misure di sicurezza. (UNI EN 292-1:1992)
- Termini di uso specialistico possono essere utilizzati e definiti in singole parti del SGSL.

3. LA POLITICA DI SALUTE E SICUREZZA SUL LAVORO

T-Systems Italia si impegna, mettendo a disposizione risorse umane, strumentali, ed economiche, a perseguire gli obiettivi di miglioramento della sicurezza e salute dei

T-Systems Italia S.p.A.

66

Modello Organizzativo di Controllo

3 novembre 2008

Documento Interno

lavoratori, come parte integrante della propria attività e come impegno strategico rispetto alle finalità più generali dell'azienda.

Rende noto questo documento e lo diffonde a tutti i soggetti dell'azienda e si impegna affinché:

- a. sia rispettata la legislazione vigente, quale presupposto fondamentale del SGSL;
- b. sia perseguita la tutela della salute e dell'integrità psicofisica dei lavoratori attraverso la predisposizione di spazi di lavoro, attrezzature e processi di elevata qualità;
- c. si considerino la sicurezza sul lavoro e i relativi risultati come parte integrante della gestione aziendale. A tale scopo:
 - i. fin dalla fase di definizione di nuove attività, o nella revisione di quelle esistenti, gli aspetti della sicurezza sono considerati contenuti essenziali;
 - ii. il sistema di gestione della sicurezza è necessariamente integrato alla struttura organizzativa aziendale;
- d. si persegua il miglioramento continuo e la prevenzione di rischi riesaminando periodicamente la politica stessa e il sistema di gestione attuato;
- e. siano fornite le risorse umane e strumentali necessarie;
- f. sia perseguito con una autonoma valutazione il "principio di precauzione", mirando alla predisposizione di misure aziendali che possono regolare gli aspetti non disciplinati dalla legislazione allo scopo di migliorare il "benessere" dei lavoratori;
- g. tutti i lavoratori siano formati, informati e sensibilizzati per svolgere i loro compiti in sicurezza e per assumere le loro responsabilità in materia di SSL;
- h. tutta la struttura aziendale partecipi, secondo le proprie attribuzioni e competenze, al raggiungimento degli obiettivi di sicurezza assegnati affinché:
 - i. i luoghi di lavoro, i metodi operativi, gli aspetti organizzativi, le attrezzature salvaguardino la salute dei lavoratori, i beni aziendali, i terzi e la comunità in cui l'azienda opera;
 - ii. l'informazione sui rischi aziendali sia diffusa a tutti i lavoratori;
 - iii. la formazione degli stessi sia effettuata ed aggiornata con specifico riferimento alla mansione svolta;
 - iv. si faccia fronte con rapidità, efficacia e diligenza a necessità emergenti nel corso delle attività lavorative;
 - v. siano promosse la cooperazione fra le varie risorse aziendali, la collaborazione con le organizzazioni imprenditoriali e con enti esterni preposti;
 - vi. siano gestite le attività anche con l'obiettivo di prevenire incidenti, infortuni e malattie professionali. Siano indirizzate a tale scopo la progettazione, la conduzione e la manutenzione, ivi comprese le operazioni di pulizia dei luoghi di lavoro e delle attrezzature.

Revisione: annuale

Documenti:

- Verbale di approvazione/revisione della politica di sicurezza

4. L' ASSETTO NORMATIVO

Il rispetto della normativa vigente costituisce presupposto fondamentale del SGSL. Per questa ragione, il Sistema prevede il censimento della normativa vigente applicabile a T-Systems e il monitoraggio continuo di aggiornamenti, modifiche, integrazioni.

Norma generale:

- Decreto legislativo 81/08 Attuazione dell'art. 1 della legge 3 agosto 2007 n. 123 in materia di tutela della salute e della sicurezza nei luoghi di lavoro

Norme specifiche:

- D.M. 37/08 Norme per la sicurezza degli impianti
- D.M. 10.3.98 Criteri generali di sicurezza antincendio e per la gestione dell'emergenza nei luoghi di lavoro
- D.Lgs. 81/08 Titolo VIII – Capo IV Protezione dei lavoratori dai rischi di esposizione a campi elettromagnetici
- Decreto legislativo 230/95 Esposizione alle radiazioni ionizzanti
- D.Lgs. 81/08 Titolo IX – Capo III Protezione dei lavoratori dai rischi connessi dall'esposizione all'amianto.

Revisione: monitoraggio continuo

Documenti:

- Legislazione aggiornata
- Verbale di verifica aggiornamento normativo

5. I DOCUMENTI DI VALUTAZIONE DEI RISCHI

La valutazione dei rischi, prescritta dalla normativa vigente, è parte integrante del presente SGSL. Le decisioni di aggiornamento e revisione del SGSL, in particolare quelle attinenti la politica di sicurezza e gli obiettivi, non possono essere assunte prescindendo da tale valutazione.

Sono redatti 9 Documenti di Valutazione dei Rischi, ciascuno per ogni sede:

- Vicenza, via degli Ontani 25
- Vicenza, Torri di Quartesolo via dell'industria 1
- Assago, Strada 2, Palazzo D Milanofiori
- Roma, Via G.V. Bona 90
- Roma, Fiumicino via Aeroporto di Fiumicino 320
- Roma, via della Maglianella 65 E/H
- Napoli, via Lauria 4 C.D.N. Isola G6
- Verona, via Sommacampagna 59/C
- Mirandola, via Statale 12 Nord 86

Per i siti presso i clienti si redige un documento che limita l'analisi alle attività svolte da T-Systems. Tale documento è poi integrato nel Documento di Valutazione dei Rischi del cliente stesso.

Revisione: annuale

Documenti:

- DVR
- Verbali di approvazione previsti dalla normativa
- Verbali di consultazione previsti dalla normativa

6. PIANIFICAZIONE DEGLI OBIETTIVI

Gli obiettivi sono definiti tenendo conto di:

- la politica aziendale di salute e sicurezza sul lavoro;
- le prescrizioni delle disposizioni normative che disciplinano la salute e la sicurezza sul lavoro;
- i Documenti di Valutazione dei Rischi.

Gli obiettivi si distinguono tra quelli che sono volti a focalizzare aspetti particolari per i quali si ritiene che l'azienda debba dedicare una specifica cura e quelli che sono volti a garantire l'efficacia e l'efficienza dell'intero sistema.

La tabella che segue descrive gli obiettivi indicando le figure o strutture coinvolte nel loro perseguimento, le risorse o le modalità da impiegare per il loro perseguimento e le modalità di verifica. Con riferimento a quest'ultima si veda anche il capitolo dedicato al monitoraggio di 1. e 2. grado.

Figure o strutture coinvolte	Risorse/modalità	Verifica
OBIETTIVI VOLTI A FOCALIZZARE ASPETTI PARTICOLARI		
Monitoraggio continuo dei vincoli normativi		
RSPD Addetto SPP	Bd, riviste, comunicazioni delle associazioni di categoria	Verifica annuale dell'aggiornamento normativo affidata al RSGSL
Forte sensibilizzazione dei lavoratori in merito ai rischi residui, con attenzione particolare ai cantieri interni		
RSPD Addetto SPP Location Manager Referenti di sito	Informazione-formazione generale e in occasione di attività di cantiere o di traslochi	Verifica annuale dell'attuazione delle iniziative di informazione-formazione affidata al RSGSL
Gestione degli infortuni		
RSPD Addetto SPP Location Manager Referenti di sito	Registro degli infortuni	Segnalazione all'OdV Verifica annuale del Registro incidenti e infortuni affidate al RSGSL
Attività di controllo del rispetto delle misure adottate dal DVR		
RSPD Addetto SPP Location Manager Referenti di sito	Definizione del piano dei controlli e delle relative modalità	Verifica dei verbali di controllo affidata al RSGSL
OBIETTIVI VOLTI A GARANTIRE L'EFFICACIA E L'EFFICIENZA DELL'INTERO SISTEMA		
Revisione periodica della Valutazione dei Rischi		
RSPD Addetto SPP	Aggiornamento dei DVR	Verifica annuale affidata all'OdV
Attuazione del piano di coinvolgimento del personale		
RSGSL	Definizione del piano di coinvolgimento del personale e sua attuazione	Verifica annuale affidata all'OdV
Attuazione dei piani di informazione, formazione e addestramento del personale		
RSPD RSGSL	Definizione dei piani di informazione, formazione e addestramento del personale e loro attuazione	Verifica annuale affidata all'OdV
Comunicazione interna ed esterna		

RSGSL	Definizione della procedura di comunicazione interna Attuazione delle modalità di comunicazione interna ed esterna	Verifica annuale affidata all'OdV
Gestione documentale		
RSP Addetto SPP RSGSL Location Manager	Gestione dei documenti del SGSL e del SSL	Verifica annuale affidata all'OdV

Revisione: annuale

Documenti:

- Verbale di approvazione/revisione degli obiettivi di sicurezza

7. ORGANIZZAZIONE DEL SISTEMA: COMPITI E RESPONSABILITA'

L'assetto organizzativo previsto dal d.lgs. 81/08 è definito nei Documenti di Valutazione dei Rischi, a cui si rimanda.

L'Amministratore Delegato individua la persona a cui affidare il ruolo di Responsabile del SGSL (RSGSL).

Il Responsabile del SGSL ha i seguenti compiti:

- assicurare che il SGSL sia definito, applicato e mantenuto nel rispetto delle Linee Guida Uni-Inail;
- riferire all'Amministratore Delegato sulle prestazioni del sistema;
- effettuare le verifiche del rispetto degli obiettivi stabiliti;
- verificare i verbali delle attività di controllo e monitoraggio;
- segnalare all'OdV
 - o eventuali incidenti, infortuni o qualsiasi evento che consideri di rilievo per la salute e sicurezza dei lavoratori;
 - o eventuali violazioni delle misure di sicurezza di cui dovesse venire a conoscenza per l'applicazione delle relative sanzioni;
- collaborare con l'OdV per le verifiche che sono affidate a quest'ultimo;
- partecipare al processo di revisione del SGSL e di definizione e pianificazione degli obiettivi.

In considerazione del fatto che il SGSL è parte del modello organizzativo adottato da T-Systems ai sensi del d.lgs. 231/01, l'OdV è parte del Sistema. A tale organo è affidata:

- l'attività di verifica (monitoraggio di 2. livello)
- l'attività sanzionatoria.

Per le altre figure previste dal SSL, quali

- RSPP,
- Addetto SPP,
- Location Manager,
- Referenti di sito,
- Medici competenti incaricati,
- Rappresentanti dei lavoratori,
- Accompagnatori di portatori di handicap in caso di emergenze
- Addetti al pronto soccorso
- Addetti antiincendio

e per le relative competenze si rimanda ai Documenti di Valutazione del Rischio.

Revisione: annuale

Documenti:

- Verbale di revisione dell'assetto organizzativo
- Organigramma previsto dai DVR

8. ORGANIZZAZIONE DEL SISTEMA: COINVOLGIMENTO DEL PERSONALE

Il coinvolgimento del personale è necessario a garantire un Sistema efficace. Il sostegno e l'impegno di tutti i partecipanti è, infatti, condizione a che quanto prescritto dal Sistema non rimanga lettera morta e diventi parte integrante della gestione aziendale.

In T-Systems il coinvolgimento del personale si realizza attraverso:

- i processi di condivisione prescritti dalla normativa;
- la partecipazione alla valutazione del rischio nel caso di introduzione di nuove attrezzature di lavoro;
- la raccolta di osservazioni in materia di SSL;
- il rilievo dato nelle riunioni aziendali qualora l'argomento trattato abbia impatto sulla sicurezza e salute dei lavoratori.

Responsabile della scelta delle forme di coinvolgimento è il RSGSL che vi dà attuazione attraverso le figure previste dall'organigramma che consideri più adeguate.

Revisione annuale

Documenti:

- Piano di coinvolgimento del personale
- Verbale di verifica dell'attuazione del piano

9. ORGANIZZAZIONE DEL SISTEMA: INFORMAZIONE, FORMAZIONE, ADDESTRAMENTO E CONSAPEVOLEZZA

L'informazione, la formazione e l'addestramento danno consapevolezza dell'importanza della SSL nel contesto produttivo aziendale. Il SGSL definisce e mantiene attive le modalità per assicurare che il personale sia ad ogni livello consapevole:

- dell'importanza della conformità delle proprie azioni rispetto alla politica ed ai requisiti del SGSL;
- delle conseguenze che la loro attività ha nei confronti della SSL;
- delle possibili conseguenze dovute ad uno scostamento da quanto fissato in materia di SSL.

Deve inoltre garantire il rispetto degli obblighi di legge in materia di informazione, formazione e addestramento dei lavoratori, nonché di informazione del personale esterno presente nei vari siti.

I piani di formazione, informazione e addestramento sono definiti dal RSPP secondo le indicazioni prescritte nei DVR. Il RSPP ne cura l'attuazione ricorrendo sia a fornitori terzi che alla struttura Academy di T-systems.

Il RSGSL è responsabile della definizione e dell'applicazione delle modalità per mantenere un'elevata consapevolezza dell'importanza delle proprie azioni ai fini del raggiungimento degli obiettivi del SSL stabiliti dall'azienda.

Revisione annuale

Documenti:

- Piani di formazione, informazione e addestramento
- Verbale di verifica di attuazione dei piani

10. ORGANIZZAZIONE DEL SISTEMA: COMUNICAZIONE, FLUSSO INFORMATIVO, COOPERAZIONE

Scopo del sistema di comunicazione è di far pervenire a tutti i soggetti dell'azienda le informazioni necessarie per consentire a ciascuno di esercitare il proprio ruolo e le proprie funzioni all'interno del SGSL. La comunicazione è interna o esterna all'azienda.

Comunicazione interna.

Da	A	Contenuto	Modalità	Azioni
Personale	RSGSL	Segnalazioni, rilievi, osservazioni, proposte relative al SGSL	Via e.mail	Risposta in tempi congrui via e.mail
Responsabili di funzione	RSPP	Segnalazione di nuove attrezzature o nuovi procedimenti lavorativi	Via email	Convocazione di riunione per la valutazione del rischio
RSGSL	Personale	Politica, obiettivi, traguardi, programmi, prestazioni, struttura organizzativa, ogni altro aspetto del SGSL	comunicati interni (anche via e.mail o sulla intranet) riunioni a gruppi omogenei, incontri singoli su particolari argomenti	
RSPP Addetto SPP Location Manager	Personale	Procedure, istruzioni operative	comunicati interni (anche via e.mail o sulla intranet) riunioni a gruppi omogenei, incontri singoli su particolari argomenti	
RSPP	RSGSL	Verbale della riunione per valutazione rischi di nuove attrezzature e nuovi procedimenti lavorativi	Via e.mail	
RSGSL	OdV	eventuali incidenti, infortuni o qualsiasi evento che consideri di rilievo per la salute e sicurezza dei lavoratori;	comunicazione scritta (anche via e.mail)	Valutazione per eventuale modifica del SGSL
RSGSL	OdV	eventuali violazioni delle misure di sicurezza di cui dovesse venire a conoscenza per l'applicazione delle relative sanzioni;	comunicazione scritta (anche via e.mail)	Valutazione per eventuale applicazione di sanzioni
RSGSL	Amministratore Delegato OdV	Verbali di monitoraggio	Comunicazione scritta (anche via e.mail)	Valutazione per eventuale modifica del SGSL
OdV	Amministratore Delegato	Verbali di monitoraggio	Comunicazione scritta (anche via e.mail)	Valutazione per eventuale modifica del SGSL

Comunicazione esterna: suddivisa in passiva e attiva.

Passiva - Ogni rilievo, osservazione, richiesta, ecc. proveniente dall'esterno e relativa a temi di SSL deve essere convogliata al RSGSL. Se si tratta di richiesta verbale deve essere tradotta in forma scritta dal ricevente.

Ogni richiesta deve essere archiviata.

Il RSGSL deve sempre rispondere entro un termine che, pur dipendendo dal tipo di richiesta, non può superare i 10 giorni.

L'invio della risposta è sempre subordinato a verifica ed approvazione dell'Amministratore Delegato.

Attiva - È responsabilità dell'Amministratore Delegato e riguarda essenzialmente:

- la politica e l'impegno dell'azienda verso la SSL;
- i risultati e i miglioramenti conseguiti;
- specifiche iniziative.

I mezzi utilizzati possono comprendere:

- la diffusione di comunicati aziendali;
- articoli sulla rivista aziendale;
- distribuzione di materiale informativo a mostre, fiere, convention, incontri pubblici, ecc.

Tra i soggetti destinatari si possono individuare almeno:

- il personale esterno (committenti, fornitori, collaboratori esterni);
- il pubblico (clienti, visitatori, soggetti interessati).

Revisione annuale

Documenti

- Verbale di verifica delle modalità di comunicazione interna ed esterna attuate
- Segnalazione all'OdV di eventuali incidenti o sinistri

11. ORGANIZZAZIONE DEL SISTEMA: DOCUMENTAZIONE

Scopo del sistema documentale è quello di garantire la conoscenza e la disponibilità delle normative, delle scelte aziendali, degli obiettivi, dei piani, e dei metodi che formano il SGSL.

Per documentazione si intende sia la documentazione del SGSL che la documentazione di SSL.

Nella documentazione del SGSL sono compresi tutti i documenti citati nel presente manuale.

I documenti si distinguono in:

- Manuale
 - o T-Systems Italia spa, Sistema di Gestione della Salute e della Sicurezza sul lavoro (vers. 0 Agosto 2008)
- Piani
 - o Piano di controlli sull'attuazione delle misure di sicurezza adottate dai DVR;
 - o Piano degli interventi per il coinvolgimento del personale;
 - o Piani di informazione, formazione e addestramento del personale
- Verbali e comunicazioni
 - o verbale di approvazione/revisione della politica di sicurezza
 - o verbale di verifica dell'aggiornamento normativo
 - o verbale di approvazione/revisione degli obiettivi di sicurezza
 - o verbale di revisione dell'assetto organizzativo
 - o verbale di verifica dell'attuazione del piano di coinvolgimento del personale
 - o verbale di verifica della comunicazione interna ed esterna attuate
 - o verbale di verifica della gestione documentale
 - o segnalazione all'OdV di eventuali incidenti o infortuni
 - o verbali di monitoraggio di primo e secondo grado
 - o verbale di valutazione del rischio nel caso di introduzione di nuove attrezzature e nuovi procedimenti lavorativi.
 - o verbale di revisione del sistema sanzionatorio
 - o verbale di riesame del Sistema.

Responsabile della documentazione del SGSL è il RSGSL.

La documentazione di SSL comprende:

- la legislazione applicabile;
- i Documenti di Valutazione dei rischi
- l'organigramma della sicurezza sul lavoro e i relativi atti di nomina:
 - o nomina del RSPP
 - o nomina dell'Addetto SPP
 - o nomina di Location Manager
 - o nomina di referenti di sito
 - o nomina medici incaricati
 - o nomina accompagnatori di portatori di handicap in caso di emergenza
 - o nomina addetti pronto soccorso
 - o nomina addetti antiincendio
 - o elenco rappresentanti dei lavoratori
- le valutazioni quali:

- esposizione al rumore
- le informative al personale quali:
 - informativa di sicurezza per accedere ai locali tecnologici (computer room e printing)
 - informativa di sicurezza per accedere ai locali tecnologici (locali impianti)
 - scheda operativa addetto evacuazione disabili
 - modalità di utilizzo estintori
- verbali
 - relazione del RSPP
 - verbale dell'elezione dei rappresentanti dei lavoratori
 - verbali di consultazione dei rappresentanti dei lavoratori
 - verbale del CdA di approvazione dei DVR
 - verbali delle riunioni periodiche.

Responsabile della documentazione del SSL è secondo le indicazioni di legge il RSPP e per quanto delegato dell'Addetto SPP.

La documentazione del SGSL e della SSL è disponibile sulla intranet aziendale.

Revisione annuale

Documenti

- Verbale di verifica della gestione documentale

12. ORGANIZZAZIONE DEL SISTEMA: INTEGRAZIONE NEI PROCESSI AZIENDALI

Al di là di quanto previsto dai DVR, la valutazione del rischio può risultare necessaria nel caso di introduzione di nuove attrezzature o nuovi procedimenti lavorativi che abbiano impatto sulla SSL.

I responsabili della funzione interessata dall'adozione di nuove attrezzature o nuovi procedimenti lavorativi comunica tale intenzione al RSPP. Questi convoca una riunione con la partecipazione di:

- addetto SPP
- location manager
- referente di sito
- rappresentanti dei lavoratori
- medici competenti incaricati

per la valutazione del rischio. Della riunione viene redatto il verbale da comunicarsi al RGSL.

Revisione: annuale

Documenti:

- Verbale riunione di valutazione del rischio

13. MONITORAGGIO

Il monitoraggio riguarda tutti gli obiettivi indicati nel presente SGSL.

Il monitoraggio si distingue in primo e secondo livello.

Il monitoraggio di primo livello ha lo scopo di tenere sotto controllo le misure preventive e protettive predisposte dall'azienda in materia di SSL. E' affidato principalmente al RSGSL.

Il monitoraggio di secondo livello ha lo scopo di stabilire se il sistema è conforme a quanto pianificato e se è correttamente applicato e mantenuto attivo. E' affidato all'Organismo di Vigilanza (OdV).

Monitoraggio di 1. Livello	Cadenza	Responsabile	Azioni
Verifica aggiornamento normativo	Annuale	RSGSL	Segnalazione al RSPP dell'aggiornamento Verifica della causa della non conformità
Verifica attuazione delle iniziative di informazione/formazione in occasione di attività di cantieri interni o di traslochi	Annuale	RSGSL	Verifica della causa della non conformità Eventuale adeguamento conseguente del sistema
Verifica registro incidenti e infortuni	Annuale	RSGSL	Valutazione del tipo di incidente o infortunio. Se esso è determinato da inefficienze del SGSL, aggiornamento del sistema.
Verifica dei verbali dell'attività di controllo delle misure adottate dai DVR	Annuale	RSGSL	Verifica della causa della non conformità. Eventuale adeguamento conseguente del sistema

Monitoraggio di 2. Livello	Cadenza	Responsabile	Azioni
Verifica della revisione periodica della valutazione dei rischi	Annuale	OdV	Segnalazione al RSPP della necessaria revisione. Verifica della causa di non conformità. Eventuale adeguamento conseguente del sistema
Verifica dell'attuazione del piano di coinvolgimento del personale	Annuale	OdV	Segnalazione al RSGSL Verifica della causa di non conformità. Eventuale aggiornamento conseguente del sistema
Verifica dell'attuazione dei piani di informazione, formazione e addestramento del personale	Annuale	OdV	Segnalazione al RSPP. Verifica della causa di non conformità. Eventuale aggiornamento conseguente del sistema
Verifica dell'attuazione delle modalità di comunicazione interna ed esterna	Annuale	OdV	Segnalazione al RSGSL. Verifica della causa di non conformità. Eventuale aggiornamento conseguente del sistema.
Verifica del sistema di gestione documentale	Annuale	OdV	Segnalazione al RSGSL o al RSPP. Verifica della causa di non conformità. Eventuale aggiornamento conseguente del sistema

Ricezione segnalazioni di infortuni o incidenti	//	OdV	Valutazione del tipo di incidente o infortunio. Se esso è determinato da inefficienze del SGSL, segnalazione al RSGSL per aggiornamento del sistema.
---	----	-----	--

I verbali di monitoraggio di primo e secondo livello sono comunicati dal RSGSL e dall'OdV all'Amministratore Delegato.

Revisione annuale

Documenti

- Verbali di monitoraggio di primo e secondo grado

14. SISTEMA SANZIONATORIO

In considerazione che il SGSL è parte integrante del modello organizzativo previsto ai sensi del d.lgs. 231/01, l'attività sanzionatoria è affidata all'OdV che agirà con i poteri e nei limiti fissati dal suddetto modello.

Nell'individuazione della pena da applicare, l'OdV considererà di estrema gravità la violazione:

- delle istruzioni di sicurezza fornite dal RSPP ed individuate dal DVR;
- degli obblighi di controllo dell'adozione di tali misure.

Revisione: annuale

Documenti:

- Verbale di revisione del sistema sanzionatorio

15. RIESAME DEL SISTEMA

Il riesame è finalizzato all'individuazione delle opportunità e delle necessità di miglioramento del sistema e/o delle prestazioni di SSL.

L'Amministratore Delegato valuta:

- se la politica, gli obiettivi e i traguardi stabiliti sono commisurati ai rischi effettivi;
- se il sistema è in grado di reagire ed adattarsi prontamente ai cambiamenti del contesto interno e esterno;
- se i risultati delle prestazioni di SSL corrispondono a quanto pianificato e se tali risultati sono mantenuti nel tempo in modo sistematico ed affidabile.

Il riesame è basato sull'analisi dei seguenti documenti del SGSL:

- risultati dei monitoraggi
- segnalazione delle non conformità e delle relative azioni correttive;
- segnalazione degli incidenti;
- azioni preventive proposte;
- verbali delle riunioni periodiche;
- risultanze delle azioni di coinvolgimento del personale;
- grado del raggiungimento degli obiettivi.

Il riesame è effettuato annualmente dall'Amministratore Delegato, sentito il RSGSL e l'OdV. I risultati del riesame sono comunicati a tutte le funzioni aziendali.

Revisione annuale

Documenti:

- Verbale di riesame del Sistema