PIANO DI PREVENZIONE DELLA CORRUZIONE 2016 -2018

parte integrante del

MODELLO DI ORGANIZZAZIONE E GESTIONE

ai sensi e per gli effetti di cui al Decreto Legislativo 8 giugno 2001, n. 231

Approvato dall'Amministratore Unico con determina N. 2016/01 in data 27/01/2016 e archiviato al n° 2016-025 del protocollo aziendale.

INDICE

PREMESSA **5**

1 NATURA E MISSION DI IT.CITY S.P.A. **6**

2 IL PIANO DI PREVENZIONE **7**

2.1 GLI OBIETTIVI 7
2.2 IL CONTENUTO 7
2.3 IL PROCESSO DI ADOZIONE DEL PIANO 8
2.4 I SOGGETTI COINVOLTI NELL'ADOZIONE DELLE MISURE 8
2.4.1 Il Responsabile dell'attuazione del Piano Triennale di prevenzione della corruzione *8*
2.4.2 Il Responsabile dell'attuazione del Programma Triennale di trasparenza e integrità *9*
2.4.3 Altri soggetti coinvolti *10*

3 AREE A MAGGIOR RISCHIO DI CORRUZIONE E PROCEDURE GESTIONALI FINALIZZATE ALLA PREVENZIONE DEI REATI **11**

3.1 REATI SOCIETARI – CORRUZIONE TRA PRIVATI 11
3.1.1. Premessa *11*
3.1.2. Fattispecie criminose rilevanti *11*
Corruzione tra privati (art. 2635 c.c.) *11*
3.1.3. Aree sensibili e processi a rischio *12*
3.2 DELITTI INFORMATICI E TRATTAMENTO ILLECITO DEI DATI 13
3.2.1. Premessa *13*
3.2.2. Descrizione della tipologia dei reati *14*
3.2.3. Aree sensibili e processi a rischio *16*
3.2.4. Il sistema dei controlli *17*
3.2.5. Delitti informatici e Codice della Privacy *21*
3.3 REATI DI CORRUZIONE 22
3.3.1 Premessa *22*
3.3.2 Fattispecie criminose rilevanti *23*
3.3.3 Aree sensibili e processi a rischio *25*
3.3.4 Il sistema dei controlli *25*

4 LE AZIONI DEL PIANO **26**

5 PROGRAMMAZIONE DELLA FORMAZIONE **27**

6 MODALITA' DI GESTIONE DELLE RISORSE UMANE E FINANZIARIE IDONEE AD IMPEDIRE LA COMMISSIONE DI REATI **28**

7 CODICE DI COMPORTAMENTO **29**

8 PROCEDURA PER L'AGGIORNAMENTO DEL PIANO **30**

9 OBBLIGHI INFORMATIVI DA PARTE DEL RESPONSABILE PER LA PREVENZIONE DELLA CORRUZIONE **30**

10 OBBLIGHI INFORMATIVI NEI CONFRONTI DEL RESPONSABILE PER LA PREVENZIONE DELLA CORRUZIONE **32**

11 TUTELA DEL DIPENDENTE CHE EFFETTUA SEGNALAZIONI DI ILLECITO (WHISTLEBLOWER) 32

12 SISTEMA DISCIPLINARE SANZIONATORIO **33**

13 PROGRAMMA TRIENNALE PER LA TRASPARENZA E L'INTEGRITA' **33**

14 RINVIO AL MODELLO ORGANIZZATIVO **33**

Revisioni			
N°	**Data**	**Descrizione**	**Rif. Paragr.**
01	27-01-2016	Prima redazione del documento	

Glossario

SOCIETÀ	Società IT.CITY S.p.A.
GRUPPO COMUNE DI PARMA	Le Società controllate dal Comune di Parma soggette ad attività di direzione e coordinamento da parte del Comune.
P.T.P.C.	Il presente documento
P.T.T.I.	Il Piano Triennale per la Trasparenza e l'Integrità
DIPENDENTI	Tutti i soggetti che intrattengono un rapporto di lavoro subordinato, di qualsivoglia natura, con la SOCIETÀ, nonché i lavoratori in distacco o in forza con contratti di lavoro parasubordinato
ORGANISMO - ODV	Organismo di Vigilanza previsto dall'art. 9 del MODELLO EX 231/2002
RESPONSABILE PER LA PREVENZIONE DELLA CORRUZIONE	L'Organismo responsabile dell'attuazione del Piano triennale di prevenzione della corruzione, nonché responsabile per la prevenzione della corruzione ex Legge 190/2012
RESPONSABILE PER L'ATTUAZIONE DELLA TRASPARENZA E L'INTEGRITÀ	L'Organismo responsabile dell'attuazione delle misure di trasparenza e integrazione previste dal D.Lgs 33/2013
COLLABORATORI	Soggetti che intrattengono con la SOCIETÀ rapporti di collaborazione senza vincolo di subordinazione, rapporti di agenzia, di rappresentanza commerciale ed altri rapporti che si concretino in una prestazione professionale, non a carattere subordinato, sia continuativa sia occasionale.
ANAC	Autorità Nazionale Anticorruzione

PREMESSA

Considerato il diffondersi di eventi di corruzione avvenuti negli ultimi anni, il Piano Nazionale Anticorruzione (P.N.A.), approvato dalla ex CIVIT (ora Autorità Nazionale Anticorruzione) ai sensi della L. 190/2012 recante le "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità della Pubblica Amministrazione", ha disposto l'obbligo, per tutti gli Enti pubblici e gli enti di diritto privato in controllo pubblico, di adottare un programma e un piano triennale in cui devono essere fissate le modalità di controllo e di prevenzione, specificamente rivolte alla prevenzione e alla repressione della corruzione.
A fine di evitare inutili ridondanze, il P.N.A. ha precisato che gli enti di diritto privato in controllo pubblico, che hanno adottato in precedenza modelli di organizzazione e gestione del rischio ai sensi del Decreto Legislativo 8 giugno 2001 n. 231, possono fare perno sugli stessi nella propria azione di prevenzione della corruzione, estendendone l'ambito di applicazione a tutti i reati contro la Pubblica Amministrazione, considerati dalla L. 190/2012, e non più soltanto a quelli espressamente previsti dal D.Lgs. 231/2001, sia dal lato attivo che passivo, tenendo conto anche del tipo di attività specificamente svolto.
L'aggiornamento 2015 al P.N.A. ha fornito inoltre, a tal proposito, ulteriori elementi integrativi ed esplicativi, in funzione del mutato quadro normativo che ha inciso sul sistema di prevenzione della corruzione a livello istituzionale.
In virtù di quanto sopra, il presente P.T.P.C. 2016-2018 costituisce parte integrante del Modello Organizzativo adottato da IT.CITY con Determina dell'Amministratore Unico in data 24/06/2014 e le misure presenti sono coordinate con le misure e gli interventi previsti dal "Modello di organizzazione e di gestione ex D.Lgs. 231/2001 e " e dal "Codice Etico", redatti in coerenza con il d.lgs. n. 231/2001.
Il presente P.T.P.C. tiene conto altresì delle Linee guida emanate dall'ANAC con determinazione n.8 del 17 giugno 2015 aventi ad oggetto "*Linee guida per l'attuazione della normativa in materia di prevenzione della corruzione e trasparenza da parte delle società e degli enti di diritto privato controllati e partecipati dalle pubbliche amministrazioni e degli enti pubblici economici*".
Dette Linee guida incidono sulla disciplina del P.T.P.C. e ne comportano una rivisitazione. Pertanto le Linee guida integrano e sostituiscono laddove non compatibili il contenuto del P.T.P.C. in materia di misure di prevenzione della corruzione e di trasparenza che devono essere adottate degli enti pubblici economici, dagli enti di diritto privato in controllo pubblico e dalle società a partecipazione pubblica.
Si è provveduto con determina dell'A.U. di IT.CITY del 25/06/2014 alla nomina del Responsabile della prevenzione della corruzione, ing. Ettore Manzali, che ha assunto anche la funzione di OdV interno e di Responsabile della Trasparenza.
Il Responsabile è tenuto a relazionarsi con il Responsabile della Trasparenza e della prevenzione della corruzione dell'ente locale (il Segretario Generale del Comune di Parma).
Le aree di rischio dell'attività di IT.CITY S.p.A. sono prevalentemente circoscritte all'area amministrativa (acquisti, fornitori, bandi ecc.) e alla gestione dei Data Base del Comune di Parma.
Per ogni area di rischio IT.CITY S.p.A. adotta una gestione di prevenzione e controllo integrando misure di tutela per gli operatori che effettueranno segnalazioni di illeciti.
Periodicamente si organizzeranno piani di aggiornamento per i Responsabili delle aree di rischio.
L'accessibilità alle informazioni pubblicate sul portale di IT.CITY adempie ai criteri di trasparenza normati nel Decreto Legislativo n. 33 del 20 aprile 2013 "Riordino della disciplina riguardante gli

obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni".
Tale decreto introduce la trasparenza come strumento per garantire l'accessibilità totale delle informazioni concernenti l'organizzazione e l'attività delle pubbliche amministrazioni, allo scopo di favorire forme diffuse di contrasto della corruzione e della cattiva amministrazione.
In quest'ottica IT.CITY S.p.A. adotta il Programma triennale per la trasparenza e l'integrità 2016-18 previsto dall'articolo 10 del Decreto trasparenza (d.lgs. n.33/2013), come modificato dal DL 90/2014 convertito dalla L. 114/2014, che prevede che le società controllate da enti pubblici redigano e approvino un P.T.T.I., che deve tra l'altro definire le misure, i modi e le iniziative per l'adempimento degli obblighi di pubblicazione, ivi comprese le misure organizzative e le procedure tecniche volte ad assicurare la regolarità e la tempestività dei flussi informativi.

1 NATURA E MISSION DI IT.CITY S.p.A.

IT.CITY S.p.a. è società "in house" del Comune di Parma che dal 2008 ne detiene la totalità delle azioni, ne indirizza la missione, approva le azioni, approva la sostenibilità degli equilibri economici e finanziari, approva i servizi erogati e verifica le azioni e le procedure.
Il controllo è altresì esercitato a mezzo di un contratto di servizio stipulato tra il Comune di Parma (Socio unico) e la Società.

IT.CITY è stata costituita nel 2000, con lo scopo di supportare la Direzione Sistemi Informativi del Comune di Parma con una struttura operativa e di gestione agile, flessibile e capace di accelerare il processo di innovazione ed informatizzazione dei processi interni all'Ente comunale e dei servizi al cittadino.

In particolare, secondo quanto previsto dall'art. 2 dello Statuto, IT.CITY ha per oggetto le attività di seguito indicate:

- la produzione e la commercializzazione di servizi aziendali, di progetti informatici, di procedure per l'automazione, la fornitura dei relativi servizi, la gestione e l'elaborazione dati e la gestione delle risorse informatiche per i soci e per i terzi, la consulenza sul sistema informativo in generale e la formazione del personale.
- l'assistenza tecnica ai clienti, la ricerca tecnica e scientifica, lo sfruttamento di brevetti e innovazioni tecnologiche relative a tutti i prodotti citati, l'ottimizzazione dei servizi interni ed esterni delle aziende, tutti i servizi e prodotti relativi alle telecomunicazioni.

IT.CITY è in grado di affrontare con successo progetti ICT complessi ed eterogenei. Il know-how aziendale consolidato ed in costante evoluzione, le capacità professionali differenti e complementari delle persone attive all'interno dell'azienda, sono fattori che consentono di approcciare con competenza molteplici progetti tecnologici indipendentemente dal loro contenuto e dagli aspetti organizzativi e di processo coinvolti.

La Società è attualmente amministrata da un Amministratore Unico, a cui spetta la legale rappresentanza, nominato dal Socio unico.

La vigilanza sull'osservanza della legge e dello Statuto, sul rispetto dei principi di corretta amministrazione, ed in particolare sulla adeguatezza dell'assetto organizzativo ed amministrativo adottato dalla Società, e sul suo concreto funzionamento, è affidata ad un *Collegio Sindacale* composto da tre Sindaci effettivi e due supplenti.

Il controllo contabile di cui all'art. 2409-bis c.c. è affidato ad una società di revisione iscritta all'apposito Registro dei Revisori Legali, istituito presso il Ministero dell'Economia e delle Finanze, individuata nella BDO Italia S.p.A.

2 IL PIANO DI PREVENZIONE

2.1 GLI OBIETTIVI

L'adozione del presente Piano è volta a prevenire ed a reprimere tutti i comportamenti che il P.N.A. ricomprende nell'ampio concetto di corruzione e, in particolare:

- a ridurre le opportunità che si manifestino casi di corruzione;
- ad aumentare la capacità di scoprire (e di reprimere) casi di corruzione;
- a creare un contesto sfavorevole alla corruzione.

2.2 IL CONTENUTO

In conformità a quanto previsto dal paragrafo B.2 dell'Allegato 1 al P.N.A., il presente Piano :

- individua le aree a maggior rischio di corruzione, incluse quelle previste nell'art. 1, comma 16, della L. 190/2012, valutate in relazione al contesto, all'attività e alle funzioni della Società;
- stabilisce la programmazione della formazione, con particolare attenzione alle aree a maggior rischio di corruzione;
- prevede procedure per l'attuazione delle decisioni della Società in relazione al rischio di fenomeni corruttivi;
- individua modalità di gestione delle risorse umane e finanziarie idonee ad impedire la commissione di reati;
- prevede l'adozione di un Codice di comportamento per i dipendenti ed i collaboratori, che includa la regolazione dei casi di conflitto di interesse per l'ambito delle funzioni ed attività amministrative;
- stabilisce la procedura per l'aggiornamento;
- prevede obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli organizzativi;
- disciplina un sistema informativo volto ad attuare il flusso delle informazioni e consentire il monitoraggio sull'implementazione del modello organizzativo da parte dell'amministrazione vigilante;
- introduce un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello organizzativo.

2.3 IL PROCESSO DI ADOZIONE DEL PIANO

Il presente *Piano* è revisionato dal Responsabile per la prevenzione della Corruzione**,** nominato con determina dell'Amministratore Unico in data 24 giugno 2014, ed è stato redatto sulla base degli indirizzi contenuti nel Piano Nazionale Anticorruzione e tenendo conto dell'esperienza di gestione e controllo della prevenzione di reati maturata da IT.CITY a seguito dell'adozione del Modello Organizzativo di cui al D. Lgs. 231/01.

2.4 I SOGGETTI COINVOLTI NELL'ADOZIONE DELLE MISURE

Con la Legge n. 190/12, lo Stato Italiano ha introdotto in primo luogo l'Autorità Nazionale Anti-corruzione e ha previsto degli Organi incaricati di svolgere, con modalità tali da assicurare un'azione coordinata, un'attività di controllo, di prevenzione e di contrasto della corruzione e dell'illegalità nella Pubblica Amministrazione.

2.4.1 Il Responsabile dell'attuazione del Piano Triennale di prevenzione della corruzione

L'art. 1 comma 7 della Legge 190/2012 prevede la nomina del responsabile della prevenzione della corruzione (di seguito Responsabile) per tutte le PA. Tale previsione è stata estesa anche a tutti gli enti pubblici economici e agli enti di diritto privato in controllo pubblico.

La scelta del responsabile della prevenzione della corruzione deve ricadere preferibilmente su dirigenti che siano titolari di ufficio di livello dirigenziale generale. Tuttavia, nelle ipotesi in cui la società sia priva di dirigenti o questi siano in numero così limitato da poter svolgere esclusivamente compiti gestionali nelle aree a rischio corruttivo, il responsabile potrà essere individuato in un funzionario che garantisca le idonee competenze. Tale soggetto non deve essere destinatario di provvedimenti giudiziali di condanna o disciplinari. Il Soggetto preposto a tale ruolo deve aver dato dimostrazione, nel tempo, di comportamento integerrimo.
Inoltre, nella scelta, occorre tener conto, quale motivo di esclusione, dell'esistenza di situazioni di conflitto di interesse, evitando, per quanto possibile, la designazione di dirigenti incaricati in settori considerati esposti al rischio.

Il *Responsabile ha i seguenti compiti*:
- elaborare (contestualmente alla relazione annuale sulla attività svolta) la proposta di *Piano* di prevenzione della corruzione, da sottoporre all'Amministratore Unico per l'approvazione;
- proporre all'Amministratore Unico modifiche del *Piano* in caso di accertamento di significative violazioni, di rilevanti mutamenti dell'organizzazione aziendale ovvero di novità normative immediatamente cogenti;
- verificare l'efficace attuazione del *Piano* e la sua idoneità ed elaborare (entro il 15 dicembre di ogni anno) la relazione annuale sull'attività svolta, assicurandone la pubblicazione;
- definire, di concerto con il Responsabile dell'area Risorse Umane, le procedure ritenute più appropriate per selezionare e formare i dipendenti destinati ad operare in settori particolarmente esposti alla corruzione;

- individuare, di concerto con il Responsabile dell'area Risorse Umane, il personale da inserire nei percorsi di formazione sui temi dell'etica e della legalità.

In virtù di quanto previsto dalla circolare del D.F.P. n. 1 del 25 gennaio 2013, il *Responsabile* deve potersi giovare di appropriate risorse umane, strumentali e finanziarie.
Al fine di adempiere ai propri compiti, il *Responsabile* può pertanto avvalersi del supporto e della cooperazione di tutti i responsabili ed i dipendenti della Società, ciascuno dei quali mantiene peraltro il personale livello di responsabilità in relazione ai compiti effettivamente svolti.
In caso di commissione, all'interno dell'Amministrazione, di un reato di corruzione accertato con sentenza passata in giudicato, il responsabile della prevenzione della corruzione risponde ai sensi dell'articolo 21 del decreto legislativo 30 marzo 2001, n.165, e successive modificazioni, nonché sul piano disciplinare, oltre che per il danno erariale e all'immagine della pubblica amministrazione, salvo che provi tutte le seguenti circostanze:

- di avere predisposto, prima della commissione del fatto, il piano triennale di prevenzione della corruzione e di aver osservato le prescrizioni relative agli obblighi di formazione del personale;
- di aver vigilato sul funzionamento e sull'osservanza del piano.

2.4.2 Il Responsabile dell'attuazione del Programma Triennale di trasparenza e integrità

L'art. 43 del decreto 33/2013 dispone che deve essere nominato il "Responsabile per la Trasparenza", individuabile nel medesimo soggetto nominato "Responsabile per la prevenzione della corruzione".
Il Responsabile per la Trasparenza svolge stabilmente un'attività di controllo sull'adempimento degli obblighi di pubblicazione previsti dalla normativa vigente, assicurando la completezza, la chiarezza e l'aggiornamento delle informazioni pubblicate.

Il responsabile per la trasparenza, in conformità con quanto previsto dall'art. 43 del D.Lgs. 33/2013:

- provvede all'aggiornamento del Programma triennale per la trasparenza e l'integrità, all'interno del quale sono previste specifiche misure di monitoraggio sull'attuazione degli obblighi di trasparenza e ulteriori misure e iniziative di promozione della trasparenza in rapporto con il Piano anticorruzione;
- controlla e assicura la regolare attuazione dell'accesso civico.

La responsabilità in caso di inadempimenti è disciplinata dagli artt. 46 e 47 del D.Lgs. 33/2013. In particolare nei casi di mancata o incompleta pubblicazione dei dati, l'inadempimento degli obblighi di pubblicazione o la mancata predisposizione del Programma triennale, costituisce elemento di valutazione della responsabilità dirigenziale. La responsabilità si esclude quando si dimostra che l'inadempimento è dipeso da causa non imputabile al responsabile.

2.4.3 Altri soggetti coinvolti

A seguito della sua approvazione, il Piano aggiornato verrà sottoposto ai seguenti soggetti:

Responsabili di Area

Affinché:

- partecipino al costante aggiornamento, segnalando aree/attività a rischio ivi non previste e proponendo le misure di prevenzione ritenute utili/necessarie;
- svolgano attività informativa nei confronti del *Responsabile*;
- partecipino al processo di gestione del rischio, osservando ed assicurando l'osservanza del presente *Piano*, che costituisce parte integrante del Modello Organizzativo adottato dalla Società ai sensi del D. Lgs. 231/01;
- adottino le misure gestionali necessarie al fine di dare attuazione al presente *Piano* e, in particolare, l'avvio di procedimenti disciplinari;
- segnalino al *Responsabile* ogni violazione del presente *Piano* e delle procedure aziendali volte a darvi attuazione e/o comunque ogni comportamento non in linea con quanto previsto nei suddetti documenti e con le regole di condotta adottate dalla Società.

Referenti

Al fine di contemperare l' intento del legislatore, di concentrare in un unico soggetto le iniziative e le responsabilità per il funzionamento dell'intero meccanismo della prevenzione con il carattere complesso dell'organizzazione amministrativa, tenendo conto anche dell'articolazione per centri di responsabilità, verrà valutata l'individuazione di Referenti per la corruzione che agiscano su richiesta del Responsabile (il quale rimane comunque il riferimento per l'implementazione dell'intera politica di prevenzione nell'ambito dell'Amministrazione e per le eventuali responsabilità che ne dovessero derivare) e, in particolare:

- contribuiscano al costante aggiornamento, segnalando aree/attività a rischio ivi non previste e proponendo le misure ritenute utili/necessarie al fine di prevenire e contrastare i fenomeni di corruzione e a controllarne il rispetto da parte dei dipendenti;
- svolgano attività informativa nei confronti del *Responsabile* e di costante monitoraggio sull'attività svolta negli ambiti di riferimento;
- segnalino al *Responsabile* ogni violazione del presente *Piano* e delle procedure aziendali volte a darvi attuazione e/o comunque ogni comportamento non in linea con quanto previsto nei suddetti documenti e con le regole di condotta adottate dalla Società.

Collegio Sindacale

Il Collegio Sindacale è relazionato dal Responsabile in merito alle attività di contrasto alla corruzione poste in essere dalla Società, e segnala al *Responsabile* ogni violazione del presente *Piano* e delle procedure aziendali, volte a darvi attuazione e/o comunque ogni comportamento non in linea con quanto previsto nei suddetti documenti e con le regole di condotta adottate dalla Società.

Dipendenti

Tutti i dipendenti partecipano al processo di gestione del rischio, osservando le misure previste nel presente *Piano*, che costituisce parte integrante del Modello Organizzativo adottato dalla So-

cietà ai sensi del D. Lgs. 231/01, segnalando eventuali situazioni di illecito e casi di personale conflitto di interesse al proprio *Responsabile di Area*.
Al personale già in servizio alla data di adozione, il Piano sarà comunicato dalla Società. Al personale neoassunto sarà consegnata copia al momento della presa di servizio.

Soggetti esterni che operano per il conseguimento degli scopi e degli obiettivi di IT.CITY

Tutti i soggetti esterni (tra cui collaboratori, consulenti, fornitori) osservano le misure contenute nel presente Piano, che costituisce parte integrante del Modello Organizzativo adottato dalla Società ai sensi del D. Lgs. 231/2001; gli stessi segnalano inoltre eventuali situazioni di illecito ovvero comportamenti non conformi a quanto previsto nel presente Piano e con le regole di condotta adottate dalla Società.

Il Socio Unico

Il Comune di Parma, in qualità di Socio Unico, verifica l'avvenuta introduzione del presente Piano nel Modello Organizzativo adottato dalla Società ex D. Lgs. 231/01 e la conformità dello stesso a quanto previsto dal P.N.A.; definisce inoltre i sistemi di raccordo finalizzati a realizzare il flusso delle informazioni nei suoi confronti di cui al successivo paragrafo 9.

3 AREE A MAGGIOR RISCHIO DI CORRUZIONE E PROCEDURE GESTIONALI FINALIZZATE ALLA PREVENZIONE DEI REATI

3.1 Reati Societari – corruzione tra privati

3.1.1. Premessa

La presente Sezione riguarda il rischio di Corruzione tra Privati, sancito dall'art. 25 del D.Lgs. 231/01, e dalla Legge Anticorruzione n. 190 del 6 novembre 2012, in vigore dal 28 novembre 2012, che estende l'ipotesi corruttiva anche se rivolta ad un privato. La sezione è suddivisa nelle seguenti parti:

1. ***Fattispecie criminose rilevanti;*** contiene la descrizione del reato di corruzione tra privati, richiamata dall'art. 25 ter del D. Lgs. 231/01 e dalla Legge 190/2012.
2. ***Aree sensibili e processi a rischio;*** identifica sinteticamente le attività a rischio nell'ambito dell'organizzazione e dell'attività aziendale in conformità a quanto prescritto dall'art. 6 comma 2 del D. Lgs. 231/01 e della Legge 190/2012.
3. ***Il sistema dei controlli***; stabilisce gli standard adottati ai fini della prevenzione degli stessi, ai sensi del Decreto.

3.1.2. Fattispecie criminose rilevanti

Di seguito e per finalità cognitive ed esplicative si riporta una breve sintesi dell'articolo 2635 del Cod. Civ. (Infedeltà a seguito di dazione o promessa di utilità), ora denominata Corruzione tra privati, richiamato dall'art. 25 ter del D. Lgs. 231/01.

Corruzione tra privati (art. 2635 c.c.)

Il reato previsto dall'articolo 2635 c.c. introduce l'ipotesi corruttiva rivolta a un privato.

I soggetti coinvolti in tale reato sono distinguibili in attivi e passivi. In particolare sono inclusi Amministratori, Direttori generali, Dirigenti preposti alla redazione dei documenti contabili societari, Sindaci e i liquidatori, Sottoposti alla direzione o alla vigilanza di uno di tali soggetti.
La condotta passiva è identificabile con l'atto di ricevere (o ricevere in promessa) denaro o altra utilità in violazione degli obblighi inerenti all'ufficio o degli obblighi di fedeltà, per un atto in danno della Società.
La condotta attiva è identificabile con l'atto del dare o promette denaro o altra utilità a uno dei soggetti sopra menzionati.
Nell art. 2635 c.c. la punibilità è estesa anche al corruttore, ovvero a colui che dà o promette denaro o altra utilità a uno dei soggetti sopra menzionati. Ai fini del regime di responsabilità amministrativa, l'art. 25-ter al comma 1, del D. Lgs. 231/2001, richiamando il comma 3 dell'art. 2635 c.c., specifica come la responsabilità ex D.lgs. 231/2001 si applica esclusivamente alla società corruttrice.

3.1.3. Aree sensibili e processi a rischio

Le aree sensibili sono stabilite in conformità con quanto definito nell'articolo 25 ter, tenendo conto dei processi e delle attività già identificate nel Decreto con riferimento ai reati societari sanzionabili e astrattamente a rischio.
L'analisi dei rischi richiama poi la natura e le caratteristiche della Società con riferimento alle attività, ai processi decisionali, ai controlli interni e ai rapporti con soggetti privati nell'ambito dei quali può essere consumato il reato.
I processi interessati riguardano le seguenti aree:

- Area acquisti, con riferimento alle attività di approvvigionamento.
- Area economico – finanziaria, con riferimento alla gestione dei processo di pagamento e incassi.
- Area amministrativa, con riferimento alla gestione della società e alle relazioni con terzi privati.
- Area personale, con riferimento al processo di assuzione.

3.1.4. Standard di controllo specifici

Processo di Approvvigionamento

Il reato di corruzione, in merito alle attività di approvvigionamento, per la società IT City, potrebbe sorgere in relazione ai rapporti che l'ufficio acquisti o l'Amministratore Unico intrattengono con i fornitori o con terze parti.
Il Responsabile acquisti e l'Amministratore Unico, ove previsto, nell'esercizio delle proprie funzioni, in conformità con quanto prescritto dalle normative di settore (D. Lgs. 12 aprile 2006 n. 163 e del DPR n. 207 del 5/10/2010) e dal regolamento interno, si occupano di:

- avviare a seguito di una manifestata esigenza interna o del Comune, la fase di selezione dei fornitori in conformità con quanto previsto dal regolamento interno;
- gestire gli ordini di acquisto in base a quanto previsto dai poteri in delega/procura o dal regolamento predisposto;
- svolgere la propria attività sulla base di un regolamento interno, che prevede anche la segregazione di responsabilità all'interno del processo;
- tenere traccia delle principali transazioni e controlli effettuati.

Processo di Pagamento e incassi

Il processo di pagamento e incassi è gestito dal Responsabile acquisti e prevede il coinvolgimento dell'Amministratore Unico, in qualità di unico procuratore della società. Su tale processo il reato di corruzione potrebbe sorgere in relazione ai rapporti di pagamento/incasso verso terzi. [1]

Il Responsabile acquisti, sulla base delle deleghe conferitegli, si occupa di:

- gestire il processo di acquisto sulla base di un regolamento interno;
- effettuare le operazioni di pagamento, sulla base di una Procedura formale e con il coinvolgimento dell'Amministratore Unico, ove previsto, che prevede anche la segregazione di responsabilità all'interno del processo e le necessarie verifiche preventive;
- tenere traccia delle principali transazioni e controlli effettuati.

Relazione con terze parti e gestione amministrativa

In tale processo rientrano tutte le attività di gestione dei rapporti con soggetti terzi fra i quali banche, legali, notai, commercialisti, consulenti, società di revisione.

La gestione di tale processo è affidata sia all'Amministratore Unico che al Responsabile dell'Area Acquisti, Controllo, Legal e Segreteria.

La sottoscrizione di documenti con soggetti terzi è responsabilità dell'Amministratore Unico. Nel compimento delle loro mansioni sia l'Amministratore Unico che il Responsabile dell'area Acquisti, Controllo, Legal e Segreteria devono rifarsi a quanto indicato nelle specifiche deleghe predisposte dalla società.

Inoltre le attività di negoziazione e stipula dei contratti/accordi devono essere eseguite in base a quanto indicato nel regolamento appositamente formalizzato, nel rispetto degli standard di segregazione dei ruoli e di tracciabilità.

Gestione delle assunzioni

Nel processo di Gestione delle assunzioni è coinvolto direttamente l'Amministratore Unico. L'intero processo di selezione e assunzione di personale di IT.CITY viene eseguito in conformità con quanto previsto del REGOLAMENTO PER IL CONTROLLO STRATEGICO E OPERATIVO DEL "GRUPPO COMUNE DI PARMA", che prevede che:

- le attività inerenti l'assunzione e l'organizzazione del personale debbano essere uniformate ai principi di carattere generale vigenti per le P.A. e alla normativa specifica destinata a regolamentare l'attività delle Società a totale o parziale partecipazione pubblica;
- fino all'adozione di propri regolamenti interni, in materia di acquisizione delle risorse umane, le singole società e/o organismi partecipati si impegnino ad applicare i regolamenti approvati dal Comune di Parma nel rispetto di quanto disposto dai principi generali in materia.

In considerazione delle dimensioni e della struttura della Società, e dei limiti imposti dal budget, non si giustifica al momento l'adozione di uno specifico regolamento interno.

3.2 Delitti Informatici e trattamento illecito dei Dati

3.2.1. Premessa

La presente Sezione riguarda il rischio di reato richiamato dall'art. 24 bis del D. Lgs. 231/01 (delitti informatici e trattamento illecito dei dati, ex L. 48/2008), che impatta anche tra aree ritenute a rischio ex 190/2012 per la Società, ed è suddivisa nei seguenti paragrafi:

[1] La quasi totalità degli incassi è relativa ai servizi forniti dal Comune di Parma.

1. ***Descrizione della tipologia dei reati***; contiene la descrizione delle fattispecie criminose rilevanti richiamate dall'art. 24 - bis;
2. ***Aree sensibili***; è volto all'Identificazione delle aree sensibili;
3. ***Il sistema dei controlli;*** procedure e modalità di verifica adottati ai fini della prevenzione dei rischi;
4. ***Delitti informatici e Codice della Privacy;*** richiama i presidi adottati in conformità alla normativa sulla privacy, estendendone la validità per la prevenzione dei reati informatici.

3.2.2. Descrizione della tipologia dei reati

Falsità in documento informatico pubblico o privato avente efficacia probatoria (Art. 491-bis cod. penale)

L'articolo di cui si tratta dispone che tutti i reati relativi alla falsità in atti disciplinati dal codice penale, tra i quali rientrano sia le falsità ideologiche che materiali, sia in atti pubblici che privati, sono punibili anche nel caso in cui riguardino non un documento cartaceo ma un documento informatico. Per completezza si segnala che si ha falsità:

- Ideologica, quando un documento contiene dichiarazioni non vere pur non essendo stato né alterato né contraffatto;
- Materiale, quando un documento non proviene dalla persona che risulta essere il mittente o di chi risulta dalla firma ovvero quando è artefatto per mezzo di aggiunte o cancellazioni successive alla sua formazione.

Accesso abusivo ad un sistema informatico o telematico (Art. 615-ter cod. penale)

Tale delitto, che è di mera condotta, si perfeziona con la violazione del domicilio informatico senza che sia necessario che l'intrusione sia effettuata allo scopo di insidiare e violare la riservatezza dei dati dei legittimi utenti.

Il reato si realizza anche nel caso in cui chi si introduce abusivamente non effettua una sottrazione materiale dei file, limitandosi ad esempio a fare una copia (accesso abusivo in copiatura) oppure limitandosi a leggere un documento (accesso abusivo di sola lettura).

Il reato inoltre si concretizza anche nel caso in cui un soggetto dopo essere entrato legittimamente in un sistema protetto di proprietà di terzi vi si trattenga contro la volontà del titolare del sistema ovvero utilizzi il sistema per finalità diverse per le quali era stato autorizzato.

Detenzione e diffusione abusiva di codici di accesso a sistemi informatici telematici. (Art. 615-quater cod. penale)

Il reato si realizza quando un soggetto 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.

Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (Art. 615-quinquies cod. pen.)

Il reato si realizza quando un soggetto, 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 procu-

ra, produce, riproduce, importa, diffonde, consegna o comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici.

Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (Art. 617-quater cod. penale)
Il reato si realizza quando un soggetto:

- intercetta fraudolentemente comunicazioni relative ad un sistema informatico o telematico intercorrenti tra più sistemi ovvero impedisca o interrompa tali comunicazioni;
- rivela, parzialmente o integralmente, mediante qualsiasi mezzo di informazione al pubblico, il contenuto delle comunicazioni.

Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (Art. 617-quinquies cod. penale)
Il reato si realizza quando qualcuno, 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.
Il reato, pertanto, si realizza con l'installazione delle apparecchiature a prescindere dal fatto che le stesse siano o meno utilizzate, purché le stesse siano potenzialmente idonee.

Danneggiamento di informazioni, dati e programmi informatici (Art. 635-bis cod. penale)
Il reato si realizza quando un soggetto distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui

Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (Art. 635-ter cod. penale)
Il reato si realizza quando un soggetto commette un fatto diretto a distruggere, deteriorate, 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.
Questo reato si differenzia dal precedente perché il danneggiamento ha ad oggetto informazioni, dati o programmi informatici dello Stato o di altro ente pubblico o comunque di pubblica utilità. Conseguentemente ricorre questa fattispecie di reato anche quando le informazioni, i dati o i programmi appartengano ad un soggetto privato ma sono destinati al soddisfacimento di un interesse di natura pubblica.

Danneggiamento di sistemi informatici e telematici (Art. 635-quater cod. penale)
Il reato si realizza quando un soggetto mediante le condotte sopra viste di cui all'art. 635-bis cod. penale ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi telematici od informatici altrui o ne ostacola gravemente il funzionamento.

Danneggiamento di sistemi informatici e telematici di pubblica utilità (Art. 635 quinquies cod. penale)

Il reato si realizza quando la condotta di cui al precedente art. 635-quater cod. penale è diretta a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi telematici od informatici di pubblica utilità od ad ostacolarne gravemente il funzionamento

Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (Art. 640-quinquies cod. penale)
Il reato si realizza quando un soggetto, che presta servizi di certificazione di firma elettronica, al fine di procurare a sé od ad altri un ingiusto profitto ovvero di arrecare ad altri un danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato.
Trattasi di reato che può essere commesso solo da parte di certificatori qualificati.

3.2.3. Aree sensibili e processi a rischio

La società risulta essere esposta al rischio di commissione dei reati descritti al paragrafo 1, nello svolgimento delle seguenti attività:

Gestione dei profili utente e del processo di autenticazione
Si tratta dell'attività svolta in merito all'assegnazione, modifica, o rimozione delle credenziali di accesso ai sistemi, affinché solo il personale autorizzato possa accedere ai sistemi con un profilo di accesso coerente con la mansione ricoperta.

Gestione del processo di creazione, trattamento e archiviazione di documenti elettronici con valore probatorio
Si tratta dell'attività volta a gestire la documentazione aziendale avente valore probatorio per quanto attiene la creazione, il trattamento e l'archiviazione con strumenti informatici.

Gestione e protezione della postazione di lavoro
Si tratta dell'attività orientata alla corretta gestione dei beni aziendali, degli apparati assegnati (ad esempio computer portatile, telefono, etc.), della posta elettronica, della sicurezza informatica e di quanto concerne la postazione di lavoro in generale (ad esempio custodia cartacea delle credenziali di accesso, etc.).

Accessi da e verso l'esterno
Si tratta dell'attività di accesso al proprio sistema o al sistema di un soggetto terzo. L'accesso può avvenire per mezzo dei sistemi interni, per mezzo di sistemi aperti (i.e. Internet) o per mezzo di sistemi di un soggetto terzo.

Gestione e protezione delle reti
Si tratta dell'attività di gestione delle reti informatiche e telematiche e della relativa sicurezza. Tale attività può essere svolta per la gestione della propria infrastruttura informatica o per la gestione dell'infrastruttura informatica di un cliente nell'ambito di uno specifico contratto di service.

Gestione degli output di sistema e dei dispositivi di memorizzazione (es. USB, CD)
Si tratta dell'attività di gestione ed utilizzo dei dispositivi di memorizzazione come Hard Disk esterni, Hard Disk portatili, Compact Disk ecc.

Sicurezza fisica
Si tratta dell'attività volta a garantire la sicurezza fisica dell'accesso alla sala CED e alle sale tecniche.

Produzione e/o vendita di programmi informatici e di servizi di installazione e manutenzione di hardware, software e reti
Si tratta dell'attività di progettazione, realizzazione, installazione di programmi informatici per i clienti ed erogazione della relativa manutenzione ed assistenza. Tali attività possono essere svolte in tutto o in parte presso la propria infrastruttura, oppure in tutto o in parte, presso l'infrastruttura del cliente.

Gestione e/o manutenzione per conto di terzi di apparecchiature, dispositivi e programmi informatici e di servizi di installazione e manutenzione di hardware, software, reti
Si tratta dell'attività di gestione e manutenzione di apparecchiature, dispositivi e programmi informatici per i clienti. Tali attività possono essere svolte in tutto o in parte presso la propria infrastruttura, oppure in tutto o in parte presso l'infrastruttura del cliente.

Gestione e/o manutenzione per proprio conto di apparecchiature, dispositivi e programmi informatici e di servizi di installazione e manutenzione di hardware, software, reti
Si tratta di attività orientate alla propria infrastruttura informatica e telematica. Consistono nella gestione e manutenzione di apparecchiature, dispositivi o programmi informatici propri. Tali attività possono essere svolte in tutto o in parte presso la propria infrastruttura, oppure in tutto o in parte presso l'infrastruttura di un soggetto terzo (fornitore esterno o appartenente al Gruppo).

3.2.4. Il sistema dei controlli

Il sistema dei controlli, predisposto da IT.CITY prevede:

- procedure di carattere generale, valide per tutte le attività di rischio,
- standard di controllo specifici.

3.2.4.1 Procedure di carattere generale

Al fine di prevenire la commissione dei reati nell'ambito delle aree, attività e operazioni a rischio precedentemente identificate, la Società elabora e adotta procedure che devono, in ogni caso, rispettare i seguenti principi generali:

- la formazione e l'attuazione delle decisioni dell'Amministratore siano disciplinate dai principi e dalle prescrizioni contenute nelle disposizioni di legge, dell'atto costitutivo, dello Statuto, del Modello, delle istruzioni e raccomandazioni delle Autorità di Vigilanza e Controllo;
- vi sia l'obbligo per l'Amministratore di comunicare tempestivamente al Collegio Sindacale e all'Organismo di vigilanza- ODV, che ne cura l'archiviazione e l'aggiornamento, tutte le informazioni relative alle cariche direttamente assunte, alle partecipazioni di cui è titolare,

direttamente o indirettamente, nonché le cessazioni o le modifiche delle medesime, le quali, per la natura o la tipologia, possono lasciare ragionevolmente prevedere l'insorgere di conflitti di interesse ai sensi dell'art. 2391 c.c.;
- siano tempestivamente e correttamente effettuate, in modo veritiero e completo, le comunicazioni previste dalla legge e dai regolamenti nei confronti delle Autorità o Organi, anche Societari, di Vigilanza o Controllo, del mercato o dei soci;
- sia prestata completa e immediata collaborazione alle Autorità o Organi di Vigilanza e Controllo, fornendo puntualmente ed esaustivamente la documentazione e le informazioni richieste;
- sia prevista l'adozione di sistemi informatici, che garantiscano la corretta e veritiera imputazione di ogni operazione al cliente, controparte o ente interessati, con precisa individuazione del beneficiario e della causale dell'operazione, con modalità tali da consentire l'individuazione del soggetto che ha disposto l'operazione o l'ha effettuata; il sistema deve prevedere l'impossibilità di modificare le registrazioni;
- nello svolgimento delle attività, i Destinatari del presente Piano sono tenuti ad attenersi, oltre che alle disposizioni contenute nei capitoli successivi, anche a quanto contenuto nei "Regolamenti", nei "Manuali di processo", nelle "Disposizioni operative", nel "Codice Etico" e nelle procedure relative alle aree di attività a rischio.

3.2.4.2 Standard di controllo specifici

Qui di seguito sono elencati gli standard di controllo individuati per le specifiche attività sensibili rilevate in ambito di sicurezza informatica.

Politiche di sicurezza

Policy: sono formalizzate le policy in materia di sicurezza del sistema informativo, finalizzate a fornire le direttive ed il supporto per la gestione della sicurezza delle informazioni in accordo con le necessità di business, la normativa e gli aspetti regolatori. Le policy chiariscono gli obiettivi, i processi ed i controlli necessari per la gestione della sicurezza informatica.
Tali policy, approvate dall'Amministratore Unico, prevedono tra l'altro:
- le modalità di diffusione e di comunicazione delle stesse anche a terzi;
- le modalità di riesame delle stesse, periodico o a seguito di cambiamenti significativi.

Organizzazione della sicurezza per gli utenti interni

Regolamento: è adottato e attuato un regolamento che definisce i ruoli e le responsabilità nella gestione delle modalità di accesso di utenti interni all'azienda e gli obblighi dei medesimi nell'utilizzo dei sistemi informatici.

Organizzazione della sicurezza per gli utenti esterni.

- Procedura: è adottata e attuata una procedura che definisce i ruoli e le responsabilità nella gestione delle modalità di accesso di utenti esterni all'azienda e gli obblighi dei medesimi nell'utilizzo dei sistemi informatici, nonché nella gestione dei rapporti con i terzi in caso di accesso, gestione, comunicazione, fornitura di prodotti/servizi per l'elaborazione dei dati e informazioni da parte degli stessi terzi.
- Clausole contrattuali: i contratti con i fornitori devono prevedere clausole specifiche per la gestione della sicurezza.

Classificazione e controllo dei beni

Procedura: sono adottate e attuate procedure che definiscono i ruoli e le responsabilità per l'identificazione e la classificazione degli "asset" aziendali (ivi inclusi dati e informazioni). Tali procedure consentono di individuare la criticità degli "asset" in termini di sicurezza informatica e sono finalizzate alla definizione degli opportuni meccanismi di protezione ed alla coerente gestione dei flussi di comunicazioni.

Sicurezza fisica e ambientale

Misure di sicurezza fisica: sono adottate e attuate le misure di sicurezza finalizzate a prevenire accessi non autorizzati, danni e interferenze ai locali e ai beni in essi contenuti tramite la messa in sicurezza delle aree e delle apparecchiature.

Gestione delle comunicazioni e dell'operatività

- Procedura: sono adottate e attuate una serie di procedure che assicurano la correttezza e la sicurezza dell'operatività dei sistemi informativi. In particolare, tali procedure disciplinano:
  - il corretto e sicuro funzionamento degli elaboratori di informazioni;
  - la protezione da software pericoloso;
  - il backup di informazioni e software;
  - la protezione dello scambio di informazioni attraverso l'uso di tutti i tipi di strumenti per la comunicazione anche con terzi;
  - gli strumenti per effettuare la tracciatura della attività eseguite sulle applicazioni, sui sistemi e sulle reti e la protezione di tali informazioni contro accessi non autorizzati;
  - una verifica dei log che registrano le attività degli utilizzatori, le eccezioni e gli eventi concernenti la sicurezza;
  - il controllo sui cambiamenti agli elaboratori e ai sistemi;
  - la gestione di dispositivi rimovibili.
- Clausole contrattuali: la correttezza e la sicurezza dell'operatività dei sistemi informativi nei rapporti con i clienti è garantita attraverso l'inserimento di specifiche clausole contrattuali che definiscono le regole operative.

Controllo degli accessi

- Procedure: sono adottate e attuate specifiche procedure che disciplinano gli accessi alle informazioni, ai sistemi informativi, alla rete, ai sistemi operativi ed alle applicazioni.
  In particolare, tali procedure prevedono:
  - l'autenticazione individuale degli utenti tramite codice identificativo dell'utente e password o altro sistema di autenticazione sicura;
  - le liste di controllo del personale abilitato all'accesso ai sistemi, nonché le autorizzazioni specifiche dei diversi utenti o categorie di utenti;
  - una procedura di registrazione per accordare e revocare l'accesso a tutti i sistemi e servizi informativi;
  - la rivisitazione dei diritti d'accesso degli utenti secondo intervalli di tempo prestabiliti usando un processo formale;
  - la destituzione dei diritti di accesso in caso di cessazione o cambiamento del tipo di rapporto che attribuiva il diritto di accesso;
  - l'accesso ai servizi di rete esclusivamente da parte degli utenti che sono stati specificatamente autorizzati e le restrizioni della capacità degli utenti di connettersi alla rete;

  - la chiusura di sessioni inattive dopo un predefinito periodo di tempo;
  - la custodia dei dispostivi di memorizzazione (ad es. chiavi USB, CD, hard disk esterni, etc.) e l'adozione di regole di *clear screen* per gli elaboratori utilizzati.
- Clausole contrattuali: gli accessi alle informazioni, ai sistemi informativi, alla rete, ai sistemi operativi e alle applicazioni nei rapporti con i clienti è garantita attraverso l'inserimento di specifiche clausole contrattuali che ne definiscono le modalità.

Gestione degli incidenti e dei problemi di sicurezza informatica

- Procedure: sono adottate e attuate specifiche procedure che definiscono le modalità per il trattamento degli incidenti e dei problemi relativi alla sicurezza informatica. In particolare, tali procedure prevedono:
  - appropriati canali gestionali per la comunicazione degli incidenti e problemi;
  - l'analisi periodica di tutti gli incidenti singoli e ricorrenti e l'individuazione della "root cause";
  - la gestione dei problemi che hanno generato uno o più incidenti, fino alla loro soluzione definitiva;
  - l'analisi di report e trend sugli incidenti e sui problemi e l'individuazione di azioni preventive;
  - appropriati canali gestionali per la comunicazione di ogni debolezza dei sistemi o servizi stessi osservata o potenziale;
  - l'analisi della documentazione disponibile sulle applicazioni e l'individuazione di debolezze che potrebbero generare problemi in futuro;
  - l'utilizzo di basi dati informative per supportare la risoluzione degli Incidenti;
  - la manutenzione della basi dati contenente informazioni su errori noti non ancora risolti, i rispettivi "workaround" e le soluzioni definitive, identificate o implementate;
  - la quantificazione e il monitoraggio dei tipi, dei volumi, dei costi legati agli incidenti e alla sicurezza informativa.
- *Clausole contrattuali*: la gestione degli incidenti e dei problemi di sicurezza nei rapporti con i clienti è garantita attraverso l'inserimento di specifiche clausole contrattuali che ne definiscono le modalità.

Audit

- Procedure: sono adottate specifiche procedure che disciplinano i ruoli, le responsabilità e le modalità operative delle attività di verifica periodica dell'efficienza ed efficacia del sistema di gestione della sicurezza informatica.
- Audit: vengono svolte attività di audit atte a verificare l'applicazione delle misure di sicurezza previste, sia nelle configurazioni dei sistema che nei singoli processi organizzativi.

Risorse umane e sicurezza

Procedure: sono adottate e attuate procedure, in conformità con quanto previsto dal Decreto Legge 31 maggio 2010 n. 78, convertito in Legge 122/2010 in materia di politiche del personale, e in base a quanto indicato all'interno del Regolamento Gruppo Comune di Parma, che prevedono:

- la valutazione (prima dell'assunzione o della stipula di un contratto) dell'esperienza delle persone destinate a svolgere attività IT, con particolare riferimento alla sicurezza dei sistemi informativi, e che tenga conto della normativa applicabile in materia, dei principi etici e della classificazione delle informazioni a cui i predetti soggetti avranno accesso;

- specifiche attività di formazione e aggiornamenti periodici sulle procedure aziendali di sicurezza informatica per tutti i dipendenti e, dove rilevante, per i terzi;
- l'obbligo di restituzione dei beni forniti per lo svolgimento dell'attività lavorativa (ad es. PC, telefoni cellulari, strumenti di autenticazione, etc.) per i dipendenti e i terzi al momento della conclusione del rapporto di lavoro e/o del contratto;
- la destituzione, per tutti i dipendenti e i terzi, dei diritti di accesso alle informazioni, ai sistemi e agli applicativi al momento della conclusione del rapporto di lavoro e/o del contratto o in caso di cambiamento della mansione svolta.

Sicurezza nell'acquisizione, sviluppo e manutenzione dei sistemi informativi

Procedura: sono adottate e attuate procedure che definiscono:

- l'identificazione di requisiti di sicurezza in fase di progettazione o modifiche dei sistemi informativi esistenti;
- la gestione dei rischi di errori, perdite, modifiche non autorizzate di informazioni trattate dalle applicazioni;
- la confidenzialità, autenticità e integrità delle informazioni;
- la sicurezza nel processo di sviluppo dei sistemi informativi.

3.2.5. Delitti informatici e Codice della Privacy

La *compliance* alle disposizioni contenute nel Codice della Privacy sul trattamento di dati personali, mediante l'impiego di risorse informatiche, rappresenta un valido strumento per impostare gli accorgimenti organizzativi utili alla prevenzione dei reati informatici. La mancanza di adeguate misure di protezione dei sistemi, degli archivi e dei dati potrebbe tradursi infatti, in accesso non autorizzato, in comunicazione e diffusione improprie, alterazione, perdita temporanea o definitiva di informazioni ecc. e creare i presupposti non solo per la violazione alla disciplina sulla privacy (trattamento illecito dei dati), ma anche di reati informatici.

La Società, pertanto, ispirandosi ai principi di necessità, correttezza e segretezza enunciati nel Codice della Privacy, per contrastare i rischi di distruzione o perdita, anche accidentale, dei dati personali oggetto del trattamento, di accesso non autorizzato e di trattamento non consentito o non conforme alle finalità della raccolta, adotta un adeguato sistema di sicurezza basato su:

- regolamentazione dei comportamenti
- formazione obbligatoria
- controllo del personale interno ed esterno

3.2.5.1 Ruoli e responsabilità

L'Amministratore Unico di IT.CITY ha nominato i Responsabili del trattamento dati ai sensi del d. lgs. 196/03, i quali, al fine di assicurare la funzionalità e il corretto impiego da parte degli utenti delle risorse informatiche:

- valutano il grado di rischio di incidenti di sicurezza informatica da parte del personale o di soggetti esterni (consulenti, agenti, ecc…);
- supportano il Titolare nel definire le modalità operative di trattamento;
- adottano idonee misure di sicurezza, di tipo organizzativo e tecnologico per garantire la disponibilità e l'integrità di sistemi informativi e di dati e per prevenire utilizzi indebiti che possono essere fonte di responsabilità;
- supportano il Titolare nell'elaborazione di un Regolamento Interno relativo a:

- utilizzo del personal computer,
- utilizzo della rete interna aziendale,
- assegnazione e gestione delle password,
- utilizzo del servizio di posta elettronica,
- accesso a particolari informazioni,
- prescrizioni sulla sicurezza dei dati e dei sistemi,
- utilizzo e conservazione dei supporti rimovibili,
- uso della rete internet e dei relativi servizi,
- policy in materia di privacy;

- osservano e garantiscono il rispetto delle disposizioni contenute nel Regolamento;
- aggiornano il Regolamento aziendale al verificarsi di eventi tali da pregiudicarne l'efficacia (modifiche legislative e regolamentari, mutamenti della struttura aziendale e delle funzioni coinvolte nello svolgimento dell'attività, ecc…);
- denunciano eventuali accessi al sistema informatico aziendale da parte di hackers;
- rendono consapevoli i dipendenti delle potenzialità degli strumenti e dei programmi elettronici implementati dall'azienda, attraverso un'attività di formazione obbligatoria che illustra:

  - i rischi che incombono sui dati;
  - le misure disponibili per prevenire eventi dannosi;
  - le responsabilità che ne derivano.

3.3 Reati di Corruzione

3.3.1 Premessa

La presente Sezione riguarda i reati di Corruzione, trattati dalla Legge Anticorruzione n. 190 del 6 novembre 2012, in vigore dal 28 novembre 2012, e contempla le ipotesi corruttive che potrebbero verificarsi nei confronti di IT.CITY.
Sebbene vi sia una sostanziale analogia tra alcuni reati-presupposto elencati dal D.Lgs. 231/2001 e quelli, propri dei pubblici ufficiali, indicati dalla L. 190/12 e dal Piano Nazionale Anticorruzione, il punto nodale è che l'ottica è diametralmente capovolta: contrariamente al dettato del D.Lgs. 231/2001, la L. 190/12, nel caso delle partecipate, intende prevenire la corruzione di tipo passivo, limitatamente alla loro attività di pubblico interesse disciplinata dal diritto nazionale o dell'Unione europea.

La sezione è suddivisa nelle seguenti parti:

- ***Fattispecie criminose rilevanti;*** contiene la descrizione dei reati di Corruzione, richiamati dalla Legge 190 del 6 novembre 2012 e dall'art. 25 del D.Lgs. 231/2001.
- ***Aree sensibili e processi a rischio;*** identifica sinteticamente le attività a rischio nell'ambito dell'organizzazione e dell'attività aziendale.
- ***Il sistema dei controlli***; stabilisce gli standard adottati ai fini della prevenzione degli stessi, ai sensi del decreto.

3.3.2 Fattispecie criminose rilevanti

Alla luce di quanto sopra, con riferimento all'attività svolta dalla Società IT.CITY S.p.A. ed ai rischi in cui potrebbe incorrere, di seguito sono stati indicati i reati ritenuti potenzialmente inerenti per la Società.

Per finalità cognitive ed esplicative si riporta una breve sintesi degli articoli 314, primo comma, 316, 317, 318, 319, 319 ter, 319 quater, 320, 322, 323, 325, 326 del Codice Penale trattati dalla legge 190 del 6 novembre 2012.

Peculato (art. 314 comma 1 c.p.)

Il reato sussiste qualora il pubblico ufficiale o l'incaricato di un pubblico servizio, che, avendo per ragione del suo ufficio o servizio il possesso o comunque la disponibilità di denaro o di altra cosa mobile altrui, se ne appropria, è punito con la reclusione da quattro a dieci anni.

Peculato mediante profitto dell'errore altrui (art. 316 c.p.)

Il reato sussiste qualora il pubblico ufficiale o l'incaricato di un pubblico servizio, il quale, nell'esercizio delle funzioni o del servizio, giovandosi dell'errore altrui, riceve o ritiene indebitamente, per sé o per un terzo, denaro od altra utilità, è punito con la reclusione da sei mesi a tre anni.

Concussione (art. 317 c.p.)

Il reato sussiste qualora 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.

Corruzione per un atto d'ufficio (art. 318 c.p.)

Il reato sussiste qualora il pubblico ufficiale, che, per compiere un atto del suo ufficio, riceve, per sé o per un terzo, in denaro o 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.

Corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.)

Il reato sussiste qualora 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.

Corruzione in atti giudiziari (art. 319-ter c.p.)

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.

Induzione indebita a dare o promettere utilità (art. 319-quater c.p.)
Il reato sussiste qualora il pubblico ufficiale o l'incaricato di pubblico servizio che abusando della propria qualità o dei propri poteri induce taluno a dare o promettere indebitamente, a lui o a un terzo, denaro o altra utilità (con previsione della reclusione da 3 a 8 anni), ma anche chi dà o promette denaro o altra utilità (con previsione della reclusione fino a 3 anni).

Corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.)
Le disposizioni dell'articolo 319 si applicano anche all'incaricato di un pubblico servizio; quelle di cui all'articolo 318 si applicano anche alla persona incaricata di un pubblico servizio, qualora rivesta la qualità di pubblico impiegato. In ogni caso, le pene sono ridotte in misura non superiore a un terzo.
In questo caso il reato sussiste qualora un soggetto che agisce per conto della società, dovesse accettare una dazione in denaro, qualsiasi altra forma di utilità o anche solo la promessa di tale utilità, da parte di un cittadino o di un membro delle amministrazioni locali, in cambio dell'erogazione di un servizio. Nel caso di terze parti il reato potrebbe essere realizzato al fine di selezionare o agevolare la scelta di un fornitore/consulente.

Istigazione alla corruzione (art. 322 c.p.)
Il reato è configurabile con la semplice offerta o promessa di 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. Tali condotte, pure se riguardano il privato, devono essere oggetto di denuncia da
parte del Pubblico Ufficiale o di Incaricato di Pubblico Servizio, pena la commissione del reato di omessa denuncia ex art. 361 c.p.

Abuso d'ufficio (art 323 c.p.)
Salvo che il fatto non costituisca un più grave reato, il pubblico ufficiale o l'incaricato di pubblico servizio che, nello svolgimento delle funzioni o del servizio, in violazione di norme di legge o di regolamento, ovvero omettendo di astenersi in presenza di un interesse proprio o di un prossimo congiunto o negli altri casi prescritti, intenzionalmente procura a sé o ad altri un ingiusto vantaggio patrimoniale ovvero arreca ad altri un danno ingiusto è punito con la reclusione da sei mesi a tre anni. La pena è aumentata nei casi in cui il vantaggio o il danno hanno un carattere di rilevante gravità.

Utilizzazione d'invenzioni o scoperte conosciute per ragioni di ufficio (art 325 c.p.)
Il reato di configura qualora il pubblico ufficiale, o l'incaricato di un pubblico servizio impiega, a proprio o altrui profitto, invenzioni o scoperte scientifiche, o nuove applicazioni industriali, che egli conosca per ragione dell'ufficio o servizio, e che debbano rimanere segrete, è punito con la reclusione da uno a cinque anni e con la multa non inferiore a lire un milione.

Rivelazione ed utilizzazione di segreti di ufficio (art 326 c.p.)
Il reato sussiste qualora il pubblico ufficiale o la persona incaricata di un pubblico servizio, che, violando i doveri inerenti alle funzioni o al servizio, o comunque abusando della sua qualità, rive-

la notizie di ufficio, le quali debbano rimanere segrete, o ne agevola in qualsiasi modo la conoscenza, è punito con la reclusione da sei mesi a tre anni.

Corruzione tra privati (Art. 25 ter del D.Lgs. 231/01)
I Reati Societari riguardanti la Corruzione tra privati previsti dall'art. 25 ter del decreto legislativo 231/2001 sono trattati nella Sezione 3.1 del presente Piano.

3.3.3 Aree sensibili e processi a rischio

Le aree sensibili sono stabilite tenendo conto di quanto ammesso dalla legge 190 del 6 novembre 2012, della natura e delle caratteristiche della Società con riferimento alle attività, ai processi decisionali, ai controlli interni e ai rapporti con soggetti privati nell'ambito dei quali può essere consumato il reato.
I processi interessati riguardano le seguenti aree:

- Area acquisti, con riferimento alle attività di approvvigionamento.
- Area economico – finanziaria, con riferimento alla gestione dei processo di pagamenti e incassi.
- Area personale, con riferimento al processo di assunzione.
- Area informatica, con riferimento al processo di gestione delle informazioni e delle Banche dati del Comune di Parma.
- Area sviluppo IT con riferimento alle attività di sviluppo software e gestione del sistema informatico del Comune di Parma.

3.3.4 Il sistema dei controlli

Al fine di limitare l'insorgere di situazioni di rischio, nello svolgimento delle proprie attività e responsabili dei vari processi impattati dai reati previsti dalla Legge 190/2012 dovranno attenersi, oltre agli standard di controllo indicati nei punti seguenti, a quanto definito nei "Regolamenti", nei "Manuali di processo", nelle "Disposizioni operative", nel "Codice Etico" e nelle procedure relative alle aree di attività a rischio

Processo di Approvvigionamento
Gli standard di controllo relativi all'area acquisti con riferimento alle attività di approvvigionamento sono definiti al paragrafo 3.1.4.2 Standard di controllo specifici della Sezione A del presente Modello,

Processo di Pagamento e incassi
Gli standard di controllo relativi all'area economico finanziaria con riferimento alla gestione del processo di pagamento e incassi sono definiti al paragrafo 3.1.4.2 Standard di controllo specifici della Sezione A del presente Modello,

Processo Gestione delle assunzioni
Gli standard di controllo relativi all'area Risorse Umane con riferimento al processo di gestione delle assunzioni sono definiti al paragrafo 3.1.4.2 Standard di controllo specifici della Sezione A del presente Modello,

Processo di gestione delle informazioni

Gli standard di controllo relativi all'area informatica con riferimento al processi di gestione delle informazioni e delle banche dati del Comune di Parma sono definiti ai paragrafi 3.2.4 della Sezione B e 3.3.4 della Sezione C del presente Modello.

Processo sviluppo IT

Gli standard di controllo relativi all'area informatica con riferimento al processi di gestione degli sviluppi e delle modifiche sui sistemi e gli applicativi informatici sono definiti ai paragrafi 3.2.4 della Sezione B e 3.3.4 della Sezione C del presente Modello.

Il Piano di Prevenzione della Corruzione insieme al "Modello di organizzazione e di gestione ex D.Lgs. 231/2001", al "Programma Triennale della Trasparenza " e al "Codice Etico", rappresentano i principali elementi guida nella definizione della pianificazione strategica nella gestione aziendale.

4 LE AZIONI DEL PIANO

IT.CITY S.p.A., al fine di rendere conforme il proprio sistema di controllo a quanto previsto dalla Legge 190/2012, per prevenire il verificarsi di attività a rischio reato ex 190/12, ha avviato un piano di adeguamento finalizzato al presidio delle attività sensibili e del verificarsi di connesse condotte illecite.

Il piano di adeguamento 190/2012 è integrato all'interno del piano di adeguamento del sistema dei controlli interni che la Società ha già avviato con riferimento a quanto previsto dal D.Lgs 231/01; il piano è reperibile presso l'OdV. In particolare di seguito si riporta lo stato di avanzamento delle misure previste dal piano.

Attività eseguite nel 2015:

- Predisposizione di un "action plan" per implementare le azioni nelle aree di miglioramento;
- Analisi delle utenze privilegiate e relative attività correttive;
- Aggiornamento delle nomine di incaricato e di responsabile ex D.Lgs 196/2003;
- Predisposizione del piano di sicurezza informatica;
- Piano di esecuzione ed esecuzione delle attività di Vulnerability Assessment;
- Predisposizione della procedura di gestione dei Backup;
- Predisposizione della procedura per la gestione degli account e erogazione della relativa formazione;
- Predisposizione delle procedure per la gestione del materiale protetto da diritti d'autore e delle licenze software e relativa formazione;
- Predisposizione della procedura per lo sviluppo e il change management e erogazione della relativa formazione;

Attività che saranno svolte a partire dal primo semestre 2016:

- Predisposizione e aggiornamento delle policy e procedure, a completamento dell'impianto documentale, per la disciplina dei principali processi ritenuti a rischio reato ex D.Lgs. 231/01 e Legge 190/12, e tra queste:
    - la procedura di gestione degli incidenti di sicurezza;
    - le procedure di gestione delle configurazioni dei server e delle postazioni di lavoro;
    - la procedura di classificazione delle informazioni;
    - la procedura di gestione della crittografia dei dati.
- Potenziamento del sistema di monitoraggio delle attività riguardanti i principali processi ritenuti a rischio reato ex D.Lgs. 231/01 e Legge 190/12;
- Revisione e aggiornamento del Regolamento Interno Aziendale.

5 PROGRAMMAZIONE DELLA FORMAZIONE

La formazione riveste un'importanza cruciale nell'ambito della prevenzione della corruzione, come affermato nella l. 190/2012 (art. 1, co. 5, lett. b); co. 9, lett. b); co. 11), e deve perseguire i seguenti obiettivi:

- sviluppare un'adeguata consapevolezza al fine di ridurre il rischio che l'azione illecita sia svolta inconsapevolmente;
- favorire la conoscenza e la condivisione degli strumenti di prevenzione in capo ai diversi soggetti che a vario titolo operano nell'ambito del processo di prevenzione;
- creare una base omogenea di conoscenza tra tutto il personale;
- fornire una competenza specifica per lo svolgimento delle attività nelle aree a più elevato rischio;
- creare una occasione di confronto tra esperienze diverse al fine di favorire la costruzione di buone pratiche, omogenee e condivise;
- diffondere gli orientamenti giurisprudenziali di specifico interesse spesso sconosciuti ai "*non addetti ai lavori*";
- contrastare l'insorgere di prassi devianti;
- diffondere valori etici, mediante l'insegnamento di principi di comportamento eticamente e giuridicamente adeguati.

La formazione viene curata dalla competente Funzione aziendale, in stretto coordinamento con il *Responsabile*.

Le attività informative/formative sono previste e realizzate:

- periodicamente, in via continuativa;
- al momento della assunzione o dell'inizio del rapporto;
- in occasione di mutamenti di mansione che implichino conoscenze più dettagliate;
- in caso di modifiche normative/organizzative che rendano necessario un tempestivo aggiornamento.

In particolare, a seguito dell'approvazione del presente *Piano,* il *Responsabile*:

- pubblicherà nel sito aziendale il testo del Piano e delle principali normative di riferimento;
- trasmetterà a tutto il personale una informativa volta a comunicare l'avvenuta adozione e pubblicazione del Piano ed a promuoverne la conoscenza ad ogni livello;
- individuerà i dipendenti che si trovano ad operare nelle aree a maggior rischio di corruzione di cui al precedente paragrafo 3;
- programmerà una serie di incontri di aggiornamento, da svolgersi frontalmente in aula, rivolti ai dipendenti di cui sopra, suddivisi in gruppi per quanto possibile omogenei, aventi ad oggetto: i contenuti del Piano, con particolare riferimento alle misure di prevenzione previste; i principali aggiornamenti normativi, con particolare riferimento alle norme di cui al Titolo II, Capo I del codice penale ed agli orientamenti giurisprudenziali di specifico interesse; i principi di comportamento suggeriti dal Codice etico adottato dalla Società, dal Decreto del Presidente della Repubblica 16 aprile 2013, n. 62 ("Regolamento recante codice di comportamento dei dipendenti pubblici, a norma dell'articolo 54 del decreto legislativo 30 marzo 2001, n. 165", di seguito, per brevità, D.P.R. 62/2013) e dalle "Linee guida in materia di codici di comportamento delle pubbliche amministrazioni (art. 54, comma 5, d. lgs. 165/2001)" emanate dalla C.I.V.I.T. con delibera n. 75 del 24 ottobre 2013.

La formazione rivolta ai responsabili di area dedicherà particolare rilievo ai "***principi per la gestione del rischio***" di cui all'Allegato 6 al P.N.A..

Nel corso del 2016 saranno programmati incontri d'aula, rivolti ai soggetti di cui sopra, finalizzati alla ripresa formativa, all'approfondimento e all'aggiornamento.

Al fine di creare una base omogenea di conoscenza tra tutto il personale, e pertanto anche tra coloro che non operano in aree individuate come a maggior rischio di corruzione, verranno predisposte e pubblicate sulla intranet aziendale una serie di comunicazioni "semplificate" volte a promuovere una diffusa conoscenza del presente *Piano*, delle misure adottate a fini preventivi nonché dei principi normativi e di interpretazione di maggiore interesse.

6 MODALITA' DI GESTIONE DELLE RISORSE UMANE E FINANZIARIE IDONEE AD IMPEDIRE LA COMMISSIONE DI REATI

IT.CITY S.p.A. ha adottato numerose procedure volte a disciplinare l'attuazione delle decisioni interne e ad attuare un efficace sistema di controllo.
Tali procedure, confluite e/o richiamate nel Modello Organizzativo adottato dalla Società ai sensi del D. Lgs. 231/2001, risultano idonee a prevenire la commissione dei c.d. ***reati presupposto*** ai fini della citata normativa e utili anche al fine di contrastare il verificarsi di fenomeni corruttivi.
Quanto alle risorse umane i dipendenti sono consapevoli dell'esistenza di procedure di controllo e coscienti del contributo che queste danno al raggiungimento degli obiettivi aziendali e dell'efficienza. Sulla base di quanto previsto dal d.lgs. 27 ottobre 2009, n.150 "Attuazione della legge 4 marzo 2009, n. 15, in materia di ottimizzazione della produttività del lavoro pubblico e di efficienza e trasparenza delle pubbliche amministrazioni", IT.CITY non è soggetta all'obbligo di

adozione del Piano delle Performance. Tuttavia nel Piano Industriale triennale sono contenuti gli obiettivi strategici della Società e nel Bilancio d'Esercizio sono contenuti i risultati perseguiti.
I premi di risultato sia a livello personale che a livello aziendale cono distribuiti annualmente secondo la contrattazione aziendale di secondo livello.

Per controlli interni si intendono tutti gli strumenti necessari o utili a indirizzare, gestire e verificare le attività dell'impresa con l'obiettivo di assicurare il rispetto delle leggi e delle procedure aziendali, proteggere i beni aziendali, gestire efficientemente le attività e fornire dati contabili e finanziari accurati e completi.
La responsabilità di creare un sistema di controllo interno efficace è comune ad ogni livello operativo. Conseguentemente tutti i dipendenti sono responsabili della definizione, attuazione e corretto funzionamento dei controlli inerenti le aree operative loro affidate.
Come previsto dal Codice Etico i responsabili di funzione sono tenuti a essere partecipi del sistema di controllo aziendale e a farne partecipi i loro collaboratori.
Quanto alle risorse finanziarie, la trasparenza contabile, come previsto dal Codice Etico si fonda sulla verità, accuratezza e completezza dell'informazione per le relative registrazioni contabili.
Ciascun dipendente è tenuto a collaborare affinché i fatti di gestione siano rappresentati correttamente e tempestivamente nella contabilità.
Per ogni operazione è conservata agli atti un'adeguata documentazione di supporto dell'attività svolta, in modo da consentire:

- l'agevole registrazione contabile;
- l'individuazione dei diversi livelli di responsabilità;
- la ricostruzione accurata dell'operazione, anche per ridurre la probabilità di errori interpretativi.

Ciascuna registrazione deve riflettere esattamente ciò che risulta dalla documentazione di supporto.
È compito di ogni dipendente far sì che la documentazione sia facilmente rintracciabile e ordinata secondo criteri logici.
I dipendenti che venissero a conoscenza di omissioni, falsificazioni, trascuratezze della contabilità o della documentazione su cui le registrazioni contabili si fondano, sono tenuti a riferire i fatti al proprio superiore o alla funzione competente.
Ogni operazione e transazione deve essere correttamente registrata, autorizzata, verificabile, legittima, coerente e congrua.
Tutte le azioni e le operazioni aziendali devono avere una registrazione adeguata e deve essere possibile la verifica del processo di decisione, autorizzazione e di svolgimento.
Rilevante ai fini che qui interessano anche il puntuale sistema delle deleghe adottato dall'Amministratore Unico della Società.

7 CODICE DI COMPORTAMENTO

Il personale di IT.CITY S.p.A. non è soggetto a rapporto di lavoro pubblico. La Società è tuttavia consapevole che lo strumento dei codici di comportamento costituisce una misura di prevenzione di fondamentale importanza, giacché le norme negli stessi contenute regolano in senso legale ed eticamente corretto il comportamento dei dipendenti, indirizzando in tal modo l'azione dell'ente intesa nel suo complesso.

In ragione di quanto sopra, con determina dell'Amministratore Unico in data 24 giugno 2014, IT.CITY ha adottato un proprio Codice Etico, allegato al Modello Organizzativo di cui al D. Lgs. 231/2001, così da farne parte integrante ed essenziale.
Il Codice Etico enuclea i principi ed i valori ai quali la Società informa lo svolgimento delle proprie attività e detta le norme di comportamento attraverso le quali detti principi e valori trovano concreta attuazione.
Il Modello Organizzativo come sopra adottato e via via aggiornato nel corso del tempo stabilisce espressamente che la violazione delle disposizioni ivi contenute costituisce illecito disciplinare e, pertanto, che anche le norme contenute nel Codice Etico fanno parte a pieno titolo del "codice disciplinare". Ai fini dell'effettività, il Modello Organizzativo prevede poi un insieme di misure dirette a sanzionare le violazioni commesse da dipendenti, dirigenti, amministratori, collaboratori, consulenti, fornitori e, più in generale, da parte di tutti coloro che a vario titolo agiscono per conto di IT.CITY, anche mediante l'introduzione di apposite clausole contrattuali espressamente stabilite.
Preso atto dell'auspicio formulato dall'Autorità Nazionale Anticorruzione con la citata delibera 75/2013, IT.CITY ha integrato il proprio Codice Etico in conformità a quanto stabilito dal P.N.A., dal relativo Allegato 1 e dal D.P.R. 62/2013, giovandosi delle linee guida definite dalla CIVIT con la delibera di cui sopra, mediante procedura aperta alla partecipazione.

8 PROCEDURA PER L'AGGIORNAMENTO DEL PIANO

Il Responsabile, in stretto contatto con l'Amministratore Unico, aggiornerà il presente Piano, mantenendo una programmazione triennale, entro il 31 gennaio di ogni anno.
La proposta di aggiornamento annuale del presente Piano verrà redatta dal Responsabile entro il 15 dicembre di ogni anno, contestualmente alla relazione annuale sulla attività svolta.
In corso d'anno, il Responsabile è tenuto a sottoporre all'Amministratore Unico le proposte di modifica del presente Piano che dovessero rendersi necessarie ed urgenti in relazione all'accertamento di significative violazioni delle prescrizioni ivi contenute, all'intervento di rilevanti mutamenti nell'organizzazione aziendale e/o all'introduzione di novità normative immediatamente cogenti.

9 OBBLIGHI INFORMATIVI DA PARTE DEL RESPONSABILE PER LA PREVENZIONE DELLA CORRUZIONE

Cosi come previsto dal Modello 231/2001, il Responsabile Anticorruzione e il Responsabile Trasparenza rientrano insieme all'OdV, tra gli Organismi di controllo definiti dalla Società.

L'Amministratore Unico di IT.CITY, in virtù di quanto espressamente previsto dal paragrafo 3.1.1 del P.N.A., ha individuato e nominato l'OdV in veste di **Responsabile per la attuazione del Piano di prevenzione della corruzione.**

In linea con quanto previsto dal Modello 231, di seguito sono indicati gli obblighi informativi del Responsabile; per la parte relativa all'OdV si rimanda al modello 231 mentre per la parte relativa

al Responsabile della Trasparenza si rimanda al Programma Triennale per la trasparenza e l'integrità.
In particolare il Responsabile per la prevenzione della Corruzione deve riferire:

- periodicamente nei confronti dell'Amministratore Unico lo stato di fatto sull'attuazione del Piano triennale anticorruzione e sul programma triennale per la trasparenza e in particolare:
    - rispetto delle prescrizioni previste, in relazione alle aree di rischio individuate;
    - eccezioni, notizie, informazioni e deviazioni dai comportamenti contenuti nel Codice Etico;
- almeno annualmente, nei confronti dell'Amministratore Unico e del Collegio Sindacale, attraverso una relazione scritta nella quale vengono illustrate le attività di monitoraggio svolte, le criticità emerse e gli eventuali interventi correttivi e/o migliorativi opportuni per l'implementazione del Piano triennale anticorruzione e del Programma triennale per la trasparenza;
- ad hoc, all'Amministratore Unico, in merito alla necessità di aggiornamento del Piano, del Programma e della mappatura delle aree a rischio in relazione a:
    - verificarsi di eventi organizzativi/operativi di rilievo;
    - cambiamenti nell'attività dell'azienda;
    - cambiamenti nella organizzazione;
    - cambiamenti normativi;
    - altri eventi o circostanze tali da modificare sostanzialmente le aree a rischio cui è esposta la Società;

  Inoltre, ai sensi dell'articolo 1, comma 14 della legge n. 190/2012, il responsabile della prevenzione della corruzione, entro il 15 dicembre di ogni anno, redige una relazione annuale che offre il rendiconto sull'efficacia delle misure di prevenzione definite dal P.T.P.C.. Questo documento dovrà essere pubblicato sul sito istituzionale, nonché trasmesso agli Organismi competenti sulla base di quanto previsto dal P.N.A..

Il *Responsabile* potrà, altresì, essere consultato in ogni momento dall'Amministratore Unico ed essere convocato dal Collegio Sindacale per riferire in merito al funzionamento ed all'osservanza del presente *Piano* o a situazioni specifiche.
Il *Responsabile* potrà, a sua volta, chiedere di essere sentito dall'Amministratore Unico e dal Collegio Sindacale ogni qualvolta lo ritenga necessario/opportuno in relazione ai compiti che gli sono affidati.
Il Responsabile è tenuto inoltre a relazionarsi con il Responsabile della Trasparenza e della prevenzione della corruzione del Socio Unico (il Segretario Generale del Comune di Parma).

10 OBBLIGHI INFORMATIVI NEI CONFRONTI DEL RESPONSABILE PER LA PREVENZIONE DELLA CORRUZIONE

Al fine di consentire al *Responsabile* il corretto e puntuale svolgimento delle delicate funzioni che gli sono assegnate, occorre garantire a tale soggetto un costante flusso di informazioni aventi ad oggetto lo stato di adozione del *Piano*, eventuali violazioni dello stesso e/o delle procedure aziendali volte a darvi attuazione e/o comunque ogni comportamento non in linea con quanto previsto nei suddetti documenti e con le regole di condotta adottate dalla Società nonché, infine, eventuali criticità rappresentate da aree/attività a rischio non previste e conseguentemente non disciplinate.
Gli obblighi informativi che fanno capo ai **soggetti a vario titolo coinvolti nella prevenzione** sono espressamente previsti nel precedente **paragrafo 2.3** (Referenti per la prevenzione, dirigenti, Collegio Sindacale, dipendenti e soggetti esterni).
Il mancato rispetto degli obblighi di cui sopra costituisce illecito disciplinare per tutti i dirigenti ed i dipendenti e non soltanto per coloro che sono stati espressamente nominati in qualità di Responsabile della funzione di monitoraggio e di controllo dell'assolvimento degli obblighi di pubblicazione. Per il Collegio Sindacale e per i soggetti esterni, invece, il mancato rispetto degli obblighi di cui sopra è, rispettivamente, fonte di responsabilità professionale e contrattuale.

11 TUTELA DEL DIPENDENTE CHE EFFETTUA SEGNALAZIONI DI ILLECITO (WHISTLEBLOWER)

Sulla base di quanto definito all'interno del Modello Organizzativo adottato da IT.CITY S.p.A. ai sensi del D.lgs. 231/2001, in merito ai flussi informativi nei confronti del Responsabile della Prevenzione della Corruzione, è previsto che le segnalazioni di illecito rivolte a tale Organismo, da esponenti aziendali o terzi, debbano essere formulate in forma scritta, e che debbano essere facilitate mediante l'istituzione di un canale informativo dedicato.

A tal fine sono stati creati i seguenti indirizzi di posta elettronica dedicati:

- Responsabile della Prevenzione della Corruzione: anticorruzione@itcity.it
- Responsabile della Trasparenza: trasparenza@itcity.it

Sempre all'interno del Modello Organizzativo è previsto altresì che le segnalazioni pervenute al Responsabile, in qualità di Organismo di controllo, siano raccolte e conservate in un apposito archivio, con accesso riservato allo stesso, e che il Responsabile agirà in modo da garantire i segnalanti contro qualsiasi forma di ritorsione, discriminazione o penalizzazione, assicurando altresì la riservatezza dell'identità del segnalante, fatti salvi gli obblighi di legge e la tutela dei diritti della Società o delle persone accusate erroneamente e/o in mala fede.
In virtù della approvazione del presente Piano, le garanzie espressamente previste per coloro che effettuano segnalazioni sono estese a tutti coloro che indirizzeranno segnalazioni al Responsabile della prevenzione, aventi ad oggetto comportamenti illeciti o, comunque, non in linea con il presente Piano e con le norme di condotta adottate dalla Società, anche soltanto potenziali e da chiunque posti in essere.

Nel corso del 2016 verranno valutati strumenti/modalità idonei a favorire le segnalazioni di illecito da parte di soggetti esterni legati alla Società da rapporti di collaborazione, consulenza, fornitura, etc.

12 SISTEMA DISCIPLINARE SANZIONATORIO

L'osservanza delle norme del Codice Etico, delle misure contenute nel presente Piano e delle prescrizioni previste dal D.Lgs. 33/2013 deve considerarsi parte essenziale delle obbligazioni contrattuali così come meglio specificato nel Modello 231, sia dal personale che dalla dirigenza, dagli Amministratori, e dai soggetti esterni contrattualmente legati a IT.CITY da rapporti di collaborazione, consulenza, fornitura etc.
La violazione delle norme degli stessi lede il rapporto di fiducia instaurato con la Società e può portare ad azioni disciplinari, legali o penali; nei casi giudicati più gravi, la violazione può comportare la risoluzione del rapporto di lavoro, se posta in essere da un dipendente, ovvero l'interruzione del rapporto, se posta in essere da un soggetto terzo.
Per tale motivo è richiesto che ciascun Soggetto coinvolto conosca le norme contenute nel Codice e nel Modello Organizzativo, oltre alle norme di riferimento che regolano l'attività svolta nell'ambito della propria funzione.
Il sistema sanzionatorio, adottato anche ai sensi art. 6, comma secondo, lett. e) D. Lgs. 231/01 deve ritenersi complementare e non alternativo al sistema disciplinare stabilito dai C.C.N.L. vigenti ed applicabili alle diverse categorie di dipendenti in forza alla Società.
L'irrogazione di sanzioni disciplinari a fronte di violazioni del presente Piano e del Codice Etico prescinde dall'eventuale instaurazione di un procedimento penale per la commissione di uno dei reati previsti dal Decreto.
Il sistema sanzionatorio e le sue applicazioni vengono costantemente monitorati dal Responsabile per la Prevenzione della Corruzione.
Nessun procedimento disciplinare potrà essere archiviato, né alcuna sanzione disciplinare potrà essere irrogata, per violazione del Modello, senza preventiva informazione e parere del Responsabile.

13 PROGRAMMA TRIENNALE PER LA TRASPARENZA E L'INTEGRITA'

Il presente Piano è stato adottato con determina dell'Amministratore Unico n. 2016/1 del 27/01/2016 congiuntamente con il Programma Triennale per la Trasparenza e l'Integrità che ne costituisce una Sezione integrante.

14 RINVIO AL MODELLO ORGANIZZATIVO

Per tutto quanto non espressamente previsto nel presente Piano si rinvia alle disposizioni contenute nel Modello Organizzativo adottato dalla Società ai sensi del D. Lgs. 231/2001, del quale costituisce parte integrante.