S.I.E.M.

SOCIETA' INTERCOMUNALE ECOLOGICA MANTOVA S.P.A.

MODELLO DI ORGANIZZAZIONE,

GESTIONE E CONTROLLO

PARTE SPECIALE E

Reati Informatici e di violazione del Diritto d'Autore

EMISSIONE E MODIFICHE			
rev.	*data*	*descrizione*	*Approvato*
-	gg/mm/anno	Prima emissione	Amministratore Unico
Il Modello di Organizzazione e Gestione Controllo, compresi i relativi Allegati, è un documento riservato e di proprietà di S.I.E.M. – Società Intercomunale Ecologica Mantovana s.p.a. In quanto tale non potrà essere divulgato a terzi, interamente o in parte, senza espressa autorizzazione da parte dell'Amministrazione Unico della Società.			

INDICE

1. TIPOLOGIA DI REATO

La presente Parte Speciale si riferisce ai:

1.1) Delitti Informatici e trattamento illecito di dati così come introdotti dalla L. 48/2008, ed elencati all'art. 24-*bis* del D. Lgs. 231/2001 (di seguito anche Decreto)

1.2) Delitti in materia di violazione del diritto d'autore così come introdotto dall'art. 7, L. 99/2009, ed elencati all'art. 25-*novies* del D.Lgs. 231/2001 (di seguito anche Decreto) con specifico riferimento ai casi che potrebbero configurarsi, in via astratta, in capo a S.I.E.M. Società Intercomunale Ecologica Mantovana s.p.a (di seguito S.I.E.M. o la Società).

1.1. DELITTI INFORMATICI E TRATTAMENTO ILLECITO DEI DATI

A seguito della ratifica ed esecuzione della "Convenzione del Consiglio d'Europa sulla Criminalità Informatica" (L.48/08 art.7) dopo l'art. 24 del D.Lgs. 231/01 è stato inserito l'art. 24-*bis* "*Delitti informatici e trattamento illecito di dati*".

Il recepimento della convenzione ha esteso la responsabilità amministrativa degli enti ai seguenti reati informatici:

- **accesso abusivo ad un sistema informatico o telematico (art. 615 ter c.p.)**
- **intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater c.p.)**
- **installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 quinquies c.p.)**
- **danneggiamento di informazioni, dati e programmi informatici (art. 635 bis c.p.)**
- **danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635 ter c.p.)**
- **danneggiamento di sistemi informatici o telematici (art. 635 quater c.p.)**

- **danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 quinquies c.p.)**
- **Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater c.p.)**
- **diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies c.p.)**
- **falsità in un documento informatico pubblico o avente efficacia probatoria (art. 491 bis c.p.)**

ESEMPI

Alterazione o intervento senza diritto su dati, informazioni o programmi contenuti su un sistema informatico o telematico di un ente pubblico, procurando a sé o ad altri un ingiusto profitto con altrui danno.

Accesso illecito ad un sistema di informazione (es. qualcuno, in violazione delle misure di sicurezza logica e fisica accede ad un sistema, senza esserne autorizzato dall'avente diritto sul sistema).

Interferenza illecita nei sistemi di informazione (es. qualcuno, consapevolmente e senza averne diritto, ostacola, interrompe il funzionamento di un sistema o ne provoca la perturbazione immettendo, danneggiando, cancellando, alterando dati informatici).

Danneggiamento di dati informatici (es. qualcuno, agendo intenzionalmente e senza diritto, cancella, danneggia, altera o rende inaccessibile dati informatici in un sistema di informazione).

1.2. DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE

L'art.7, Legge 99/2009 ha introdotto all'art. 25-novies del D.Lgs.231/2001 i "*Delitti in materia di violazione del diritto d'autore"* in base ai quali:

- **art. 171 L. 633/41 e s.m.i.**

Chiunque, senza averne diritto, a qualsiasi scopo e in qualsiasi forma:

a) riproduce, trascrive, recita in pubblico, diffonde, vende o mette in vendita o pone altrimenti in commercio un'opera altrui o ne rivela il contenuto prima che sia reso pubblico, o introduce e mette in circolazione nello Stato esemplari prodotti all'estero contrariamente alla legge italiana; [.....]

- **art. 171-bis L. 633/93 e s.m.i.**

Chiunque abusivamente duplica, per trarne profitto, programmi per elaboratore o ai medesimi fini importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale [.....] è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da euro 2.582 a euro 15.493.

ESEMPI

Installazione e utilizzo di programmi software illegali e/o contraffatti non approvati dalla Società e non correlati all'attività professionale espletata da parte dei destinatari e degli utilizzatori.

Utilizzo di software privi delle necessarie autorizzazioni/licenze d'uso.

2. INDIVIDUAZIONE DEI PROCESSI E ATTIVITA' SENSIBILI

Le attività nelle quali possono essere commessi, in via astratta e teorica, i reati informatici e trattati in modo illecito i dati aziendali informatici sono proprie di ogni ambito aziendale che utilizza le tecnologie dell'informazione.
Pertanto i principi di comportamento espressi nella presente Parte Speciale devono essere conosciuti e rispettati da tutti i dipendenti e i collaboratori della Società.

Le attività nelle quali è maggiore il rischio che siano posti in essere i comportamenti illeciti come sopra descritti è la gestione e l'utilizzo dei **sistemi informatici e delle informazioni aziendali**. In particolare:

- ✓ gestione dei sistemi informatici
- ✓ gestione dei profili utenti e del relativo processo di autenticazione
- ✓ protezione delle postazioni di lavoro
- ✓ gestione degli accessi verso l'esterno
- ✓ protezione delle reti

Con riferimento ai delitti in materia di **violazione del diritto d'autore**, l'area di attività a rischio individuata riguarda:

- ✓ l'installazione e l'utilizzo di software non autorizzati (es.: software, banche dati)

3. PRINCIPI DI COMPORTAMENTO

La presente Parte Speciale si riferisce, specificamente, a tutti coloro che, in ambito S.I.E.M. utilizzano e/o gestiscono dati informatici e/o sistemi informatici.

Nello svolgimento delle proprie attività e nei limiti dei rispettivi compiti, funzioni e responsabilità, i Destinatari devono rispettare le previsioni e le prescrizioni del Modello adottato da S.I.E.M. Ed in particolare:

1) la normativa vigente applicabile sulla materia oggetto della presente Parte Speciale
2) il Codice Etico
3) i Principi Generali di Comportamento
4) le Procedure Aziendali collegate ai Processi Sensibili.

In particolare ai Destinatari del Modello e specificamente di questa Parte Speciale, è fatto divieto:

- *porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle considerate dal D. Lgs 231/2001;*
- *porre in essere, collaborare o dare causa alla realizzazione di comportamenti che, sebbene non costituiscano di per sé fattispecie di reato rientranti tra quelle considerate dal D. Lgs 231/2001, possano potenzialmente diventarlo;*
- *sono altresì vietate le violazioni ai principi e alle prescrizioni contenute nei protocolli e/o nelle procedure aziendali che potrebbero comportare rischi di commissione dei suddetti reati.*

In relazione ai **reati informatici e trattamento illecito dei dati** :

a) ogni utente è tenuto alla segnalazione al vertice aziendale di eventuali incidenti di sicurezza (anche concernenti attacchi al sistema informatico da parte di *hacker* esterni) mettendo a disposizione e archiviando tutta la documentazione relativa all'incidente;

b) è vietato falsificare, in tutto o in parte, un documento informatico avente efficacia probatoria o di alterarne uno vero, con particolare riferimento a procedure amministrative, quali certificati e/o autorizzazioni;

c) è vietato inserire dati o informazioni non veritiere quando queste sono destinate ad elaborazioni informatizzate, elenchi o registri elettronici;

d) ogni utente è responsabile del corretto utilizzo delle risorse informatiche a lui assegnate (ad esempio personal computer fissi o portatili), che devono essere utilizzate esclusivamente per l'espletamento della propria attività. Tali risorse devono essere conservate in modo appropriato e la Società dovrà essere tempestivamente informata di eventuali furti o danneggiamenti;

e) ogni utente è responsabile del corretto utilizzo delle reti informatiche aziendali quali aree di condivisione strettamente professionale;

f) è previsto il divieto di installazione, downloading e/o utilizzo di programmi e tools informatici che permettano di alterare, contraffare, attestare falsamente, sopprimere, distruggere e/o occultare documenti informatici pubblici o privati, ovvero che consentano l'introduzione abusiva all'interno di sistemi informatici o telematici protetti da misure di sicurezza o che permettano la permanenza (senza averne l'autorizzazione) al loro interno, in violazione delle misure poste a presidio degli stessi;

g) è fatto divieto di reperire, diffondere, condividere e/o comunicare password, chiavi di accesso o altri mezzi idonei a permettere le condotte di cui al punto precedente;

h) è fatto divieto di utilizzare software e/o hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;

i) è fatto divieto di accesso in maniera non autorizzata ai sistemi informativi della Pubblica Amministrazione o di terzi per ottenere e/o modificare informazioni a vantaggio della Società;

j) è fatto divieto di alterare, mediante l'utilizzo di firma elettronica altrui o comunque in qualsiasi modo, documenti informatici;

k) è fatto divieto di utilizzo, installazione, downloading di programmi o tools informatici che consentano di modificare, alterare e/o nascondere informazioni relative al *mittente* di informazioni, documenti e dati informatici;

l) qualora sia previsto il coinvolgimento di soggetti terzi/outsourcer nella gestione dei sistemi informatici e del patrimonio informativo tali soggetti devono impegnarsi ad operare nel rispetto della normativa vigente e delle disposizioni previste in materia dal Modello di S.I.E.M. (es.: Codice Etico, Principi Generali di Comportamento).

In relazione ai **Reati di violazione del diritto d'autore**:

m) è dovuto il rispetto delle licenze, dei diritti d'autore e di tutte le leggi e regolamenti locali, nazionali ed internazionali che tutelano la proprietà intellettuale;

n) è vietato distribuire, commercializzare ed utilizzare programmi, materiale audio, video fotografico su cui la Società non abbia acquisito o non possa acquisire un titolo di proprietà o una licenza d'uso.

Relativamente a questi punti S.I.E.M. **si impegna** a:

- ✓ prevedere il divieto di copiare supporti di memorizzazione, sottoposti a licenze d'uso;
- ✓ prevedere il divieto di duplicare e/o diffondere in qualsiasi forma programmi, utilities, archivi o database soggetti a tutela del diritto d'autore, se non nelle forme e per gli scopi di servizio per i quali sono stati assegnati.

4. PRESIDI E PROTOCOLLI DI PREVENZIONE

Al fine di assicurare il rispetto dei principi di comportamento e più in generale individuare opportune modalità di prevenzione nella realizzazione di comportamenti illeciti a rischio reato, S.I.E.M. promuove o predispone adeguati presidi al cui rispetto sono tenuti i Destinatari del Modello nello svolgimento delle proprie attività e nei limiti dei rispettivi compiti, funzioni e responsabilità.

Con particolare riferimento ai rischi, alle aree di attività e ai processi indicati nel presente documento, oltre a quanto già indicato nel precedente paragrafo i principali presidi e protocolli di comportamento individuati e definiti da S.I.E.M. sono:

Rapporti di service

- **Formalizzato rapporto di servizio** con società esterna a supporto dell'attività di gestione, aggiornamento e controllo dei sistemi informativi
- Sistema di comunicazione e "**vincoli contrattuali**" in tema di 231 per i consulenti, i fornitori di servizi ed i partner della Società

Strumenti organizzativi

Ruoli e responsabilità definiti

- "profili abilitativi" definiti in base ai ruoli e funzioni svolte all'interno della Società

Segregazione dei compiti

- le attività di installazione, implementazione e modifica dei software, gestione delle procedure informatiche, controllo degli accessi fisici, logici e di sicurezza sono demandati all'Amministratore di Sistema (in outsourcing) a garanzia della corretta gestione e del presidio continuativo sul processo di gestione e utilizzo dei sistemi informativi da parte degli utenti.

5. FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA

I controlli svolti dall'Organismo di Vigilanza saranno diretti a verificare la conformità delle attività aziendali in relazione ai principi espressi nel presente documento e, in particolare, ai protocolli e alle procedure interne in essere e a quelle che saranno adottate in attuazione del presente documento.

A tal fine, si ribadisce che all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante inerente le fattispecie di Attività Sensibili.

E' compito della Società garantire la predisposizione e l'aggiornamento di adeguati flussi informativi verso l'OdV nell'ambito delle attività sensibili descritte nella presente Parte Speciale, in particolare:

- comunicare eventuali distonie comportamentali rispetto a quanto previsto dalla presente Parte Speciale.

I Destinatari del Modello devono segnalare all'Organismo di Vigilanza ogni comportamento a rischio reato e/o contrario ai principi etico-comportamentali previsti dal Modello, in tutte le fasi del processo qui indicato. Le segnalazioni saranno prese in considerazione solo se opportunamente circostanziate.

- I soggetti che ricoprono funzioni apicali e che siano responsabili di tali processi, ove, nell'espletamento del proprio dovere di vigilanza, non abbiano ravvisato la necessità di effettuare alcuna segnalazione, formalizzano tale verifica attraverso apposita dichiarazione da inviare all'OdV con cadenza semestrale.

La Società e l'Organismo di Vigilanza tutelano i soggetti da ogni effetto pregiudizievole che possa derivare dalla segnalazione.

L'Organismo di Vigilanza assicura la riservatezza dell'identità dei segnalanti, fatti salvi gli obblighi di legge.