

ETAMBIENTE S.P.A.

MODELLO DI ORGANIZZAZIONE,
GESTIONE E CONTROLLO EX
D. LGS. 8 GIUGNO 2001 N. 231

PARTE SPECIALE B

REATI INFORMATICI
(ART. 24 BIS)

ETAMBIENTE S.P.A.
VIA DI ROCCA TEDALDA, 435 - 50136 – FIRENZE (FI)
PARTITA IVA: 06870020481

INDICE

LE FATTISPECIE DI REATO	3
IDENTIFICAZIONE DELLE ATTIVITA' A RISCHIO REATO	5
PRINCIPI GENERALI DI COMPORTAMENTO.....	6
PROCEDURE DI CONTROLLO	7

LE FATTISPECIE DI REATO

La presente Parte Speciale si riferisce ai reati informatici, richiamati dall'art. 24 bis del D. Lgs 231/2001, e in particolare riporta le singole fattispecie di reato considerate rilevanti per la responsabilità amministrativa di **ETAmbiente S.p.A.**. Individua inoltre le cosiddette Attività "Sensibili" (quelle dove è teoricamente possibile la commissione del reato e che sono state individuate nell'ambito dell'attività di analisi dei rischi) specificando i principi comportamentali e i presidi di controllo operativi per l'organizzazione, lo svolgimento e la gestione delle operazioni svolte nell'ambito delle sopracitate Attività "Sensibili".

In considerazione dell'analisi dei rischi effettuata, sono risultati potenzialmente realizzabili nel contesto aziendale di **ETAmbiente S.p.A.** i seguenti reati:

- **ACCESSO ABUSIVO AD UN SISTEMA INFORMATICO O TELEMATICO (ART. 615 TER C.P.)**

Tale reato si realizza quando un soggetto abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha diritto ad escluderlo.

L'accesso è abusivo poiché effettuato contro la volontà del titolare del sistema, la quale può essere implicitamente manifestata tramite la predisposizione di protezioni che inibiscano a terzi l'accesso al sistema stesso.

- **DETENZIONE E DIFFUSIONE ABUSIVA DI CODICI DI ACCESSO A SISTEMI INFORMATICI O TELEMATICI (ART. 615 QUATER C.P.)**

Tale reato si realizza quando un soggetto, al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso di un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo.

Questo delitto si integra sia nel caso in cui il soggetto che sia in possesso legittimamente dei dispositivi di cui sopra (operatore di sistema) li comunichi senza autorizzazione a terzi soggetti, sia nel caso in cui tale soggetto si procuri illecitamente uno di tali dispositivi.

L'art. 615 quater, inoltre, punisce chi rilascia istruzioni o indicazioni che rendano possibile la ricostruzione del codice di accesso oppure il superamento delle misure di sicurezza.

- **DANNEGGIAMENTO DI INFORMAZIONI, DATI E PROGRAMMI INFORMATICI (ART. 635 BIS C.P.)**

Tale fattispecie reato si realizza, salvo che il fatto costituisca più grave reato, 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 C.P.)**

Il delitto, che può essere commesso da chiunque, consiste, salvo che il fatto costituisca più grave reato, nella commissione di un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico.

- **DANNEGGIAMENTO DI SISTEMI INFORMATICI O TELEMATICI (ART. 635 QUATER C.P.)**

Questo reato si realizza quando un soggetto attraverso il danneggiamento di dati, informazioni e programmi informatici, oppure attraverso l'introduzione o la trasmissione di dati, informazioni e programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento.

- **DANNEGGIAMENTO DI SISTEMI INFORMATICI E TELEMATICI DI PUBBLICO INTERESSE (ART. 635 - QUINQUIES C.P.)**

Il delitto è commesso se il fatto di cui all'art. 635 - quater c.p. è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento. La pena associata a tale fattispecie è quella della reclusione da uno a quattro anni. Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni.

- **ESTORSIONE (ART. 629 CO. 3 C.P.)**

Il delitto è commesso da chiunque, mediante le condotte di cui agli articoli 615-ter, 617-quater, 617-sexies, 635-bis, 635-quater e 635-quinquies ovvero con la minaccia di compierle, costringe taluno a fare o ad omettere qualche cosa, procurando a sé o ad altri un ingiusto profitto con altrui danno.

IDENTIFICAZIONE DELLE ATTIVITA' A RISCHIO REATO

Le attività che la Società ha individuato come sensibili, nell'ambito dei delitti informatici, sono di seguito riepilogate:

- Accesso ai sistemi informatici aziendali o di terze parti, che contengono, a titolo esemplificativo e non esaustivo:
 - informazioni riservate di enti pubblici
 - informazioni bancarie
 - disegni / progetti.
- Acquisizione, detenzione e gestione abusiva di credenziali di accesso (password) a sistemi aziendali o di terze parti.
- Gestione di strumenti e dispositivi e programmi, da parte di soggetti aziendali e amministratori di sistema, mediante i quali possono:
 - essere intercettate informazioni rilevanti di terze parti o impedita comunicazioni;
 - danneggiare un sistema informatico o telematico, nell'ambito delle strutture di un concorrente.
- Falsificazione di documenti informatici relativi, ad esempio, a rendicontazione in formato elettronico di attività e/o a attestazioni elettroniche di qualifiche o requisiti della Società
- Gestione delle comunicazioni verso la Pubblica Amministrazione derivanti dagli obblighi di legge.

PRINCIPI GENERALI DI COMPORTAMENTO

Coerentemente con i principi deontologici aziendali di cui alla Parte Generale del Modello Organizzativo ex D. Lgs.231/2001 e del Codice Etico adottato dalla Società, tutti i Destinatari del Modello che, a qualunque titolo, siano stati designati o incaricati alla gestione e manutenzione dei *server*, delle banche dati, delle applicazioni, dei *client* e delle reti di telecomunicazione, nonché a tutti coloro che abbiano avuto assegnate *password* e chiavi di accesso al sistema informativo aziendale sono tenuti ad osservare i seguenti principi di comportamento e controllo:

- il personale si deve astenere da qualsiasi condotta che possa compromettere la riservatezza e l'integrità delle informazioni e dei dati aziendali e dei terzi, ed in particolare si premura di non lasciare incustoditi i propri sistemi informatici e bloccarli, qualora si allontanano dalla postazione di lavoro, con i propri codici di accesso ovvero di spegnere il computer e tutte le periferiche al termine del turno di lavoro;
- il personale si astiene da qualsiasi condotta diretta a superare o aggirare le protezioni del sistema informatico aziendale o altrui;
- il personale si impegna a sottoscrivere lo specifico documento relativo al corretto utilizzo delle risorse informatiche aziendali;
- il personale conserva i codici identificativi assegnati, astenendosi dal comunicarli a terzi, che in tal modo potrebbero accedere abusivamente a dati aziendali riservati;
- il personale non può installare programmi senza aver preventivamente informato la funzione aziendale preposta alla gestione della sicurezza informatica;
- il personale non può utilizzare connessioni alternative rispetto a quelle fornite dalla Società nell'espletamento dell'attività lavorativa resa in suo favore;
- i contratti/ordini di acquisto e lettere di incarico con i professionisti/consulenti a cui è stata esternalizzata la gestione dell'infrastruttura tecnologica, o parte di essa, contengono adeguate clausole di tutela della sicurezza delle informazioni, nonché informativa sulle norme comportamentali adottate dalla Società relativamente al Codice Etico, nonché sulle conseguenze che comportamenti contrari alle previsioni del Codice Etico, ai principi comportamentali che ispirano la Società e alle normative vigenti, possono avere con riguardo ai rapporti contrattuali.

PROCEDURE DI CONTROLLO

Ad integrazione delle regole comportamentali di carattere generale sopraindicate, si riportano di seguito ulteriori presidi di controllo operativi a prevenzione della commissione dei reati informatici, con particolare riferimento ai processi sensibili/strumentale alla commissione dei reati quali:

Gestione della documentazione

Di seguito sono indicati i presidi di controllo operativi, relativi ai processi sensibili/strumentali all'interno dei quali potrebbero potenzialmente essere perpetrati, i reati sopra elencati.

- **Gestione delle risorse materiali (ICT):**

- il personale accede al sistema informativo aziendale unicamente attraverso il profilo identificativo assegnato, attraverso user ID e password strutturate sulle base di un adeguato livello di complessità;
- sono definiti meccanismi di monitoraggio del traffico e di tracciatura degli eventi di sicurezza sulle reti, da parte degli utenti e degli amministratori di sistema, nel rispetto della segregazione dei compiti (ad esempio: accessi anomali per frequenza, modalità, temporalità);
- è definita una policy formale che regoli l'utilizzo della strumentazione tecnologica (e.g. laptop, telefoni) concessa in dotazione al personale della Società.
- sono definiti formalmente i requisiti di autenticazione ai sistemi per l'accesso ai dati e per l'assegnazione dell'accesso remoto agli stessi da parte di soggetti terzi quali consulenti e fornitori;
- sono definite procedure formali per la gestione del processo di dismissione delle utenze cessate;
- è definita una policy che disciplina gli accessi fisici alle sale server aziendali;
- gli amministratori di sistema sono muniti di proprie credenziali di autenticazione e gli accessi sugli applicativi aziendali;
- sono definiti i criteri e le modalità per l'assegnazione, la modifica e la cancellazione dei profili utente;
- l'accesso alle informazioni che risiedono sui server e sulle banche dati aziendali, ivi inclusi i client, è limitato da strumenti di autenticazione;
- la rete di trasmissione dati aziendale è protetta da adeguati strumenti di limitazione degli accessi (*firewall* e *proxy*);
- il server e i laptop aziendali sono protetti da programmi antivirus, aggiornati in modo automatico, contro il rischio di intrusione;
- sono previste procedure di controllo dell'installazione di software sui sistemi operativi da parte dei dipendenti;
- sono definite regole per la navigazione in Internet che includono tra le altre l'utilizzo della rete al solo fine lavorativo, il divieto di scarico di software nelle strutture informative aziendali (share, etc.) e di connessione a siti segnalati anche da specifica messaggistica di *alert*.