PROCEDURA 9
GESTIONE DELLE
ATTIVITA' INFORMATICHE

INDICE:

1. Obiettivi

La presente procedura ha l'obiettivo di definire ruoli e responsabilità, nonché dettare protocolli di prevenzione e controllo, in relazione alla Gestione delle Attività Informatiche al fine di prevenire, nell'esecuzione di tale attività, la commissione degli illeciti previsti dal D.lgs. 231/2001.

In particolare, la presente procedura intende prevenire il verificarsi delle fattispecie di reato previste nei seguenti articoli del D.lgs. 231/01 (a titolo riassuntivo, rimandandosi per l'analisi dettagliata alla parte speciale del presente MOG 231):

- art. 640 ter c.p. – frode informatica (art. 24 D.lgs. 231/01)
- delitti informatici e trattamento illecito di dati (art. 24 bis D.lgs. 231/01);
- delitti in materia di violazione del diritto d'autore (art. 25 novies D.lgs. 231/01);
- delitti in materia di strumento di pagamento diversi dai contanti e trasferimento fraudolento di valori (art. 25 octies, D.Lgs. 231/01).

La presente procedura è altresì volta a prevenire il reato di cui all'art. 416 c.p. (associazione per delinquere), laddove finalizzato alla commissione dei reati di cui sopra.

2. Destinatari

I reati di cd. "criminalità informatica" (quali quelli in precedenza indicati) prevedono quale presupposto la disponibilità di un terminale e la concreta disponibilità di accesso alle postazioni di lavoro.

Pertanto, i Destinatari della presente procedura vanno individuati in tutti coloro che utilizzano un personal computer e/o hanno accesso alla posta elettronica e/o utilizzano programmi informatici e/o hanno accesso ad internet

3. Processi aziendali coinvolti

I Destinatari della presente procedura, per quanto rileva ai fini della prevenzione dei reati pocanzi menzionati, partecipano alla gestione delle attività informatiche principalmente (ed a titolo esemplificativo) attraverso i seguenti processi aziendali:

- ordinaria e straordinaria amministrazione
- coordinamento e gestione delle attività aziendali
- gestione dei sistemi informativi
- gestione della procedura espropriativa
- gestione dei dati personali
- svolgimento dei processi che richiedono l'utilizzo dello strumento informatico (gestione del profilo utente e del processo di autenticazione, gestione e protezione della postazione di lavoro, gestione degli accessi verso l'esterno, gestione e protezione delle reti sicurezza fisica dei sistemi informatici).

4. Protocolli di prevenzione

Ogni attività svolta con l'ausilio del mezzo informatico deve avvenire nel rispetto della normativa vigente, della normativa in materia di diritto d'autore, copyright e privacy, nonché nel rispetto di tutta la normativa nazionale ed internazionale concernente l'utilizzo dei mezzi informatici.

La società adotta misure tecniche ed organizzative adeguate volte ad attuare in maniera efficace i principi di protezione dei dati. In particolare, la società assicura:

- il trattamento dei dati personali in modo lecito, corretto e trasparente,
- la raccolta dei dati personali per finalità determinate esplicite e legittime,
- la conservazione dei dati personali in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati,
- il trattamento in maniera da garantire un'adeguata sicurezza anche mediante misure tecniche e organizzative atte a evitare trattamenti non autorizzati o illeciti, nonché la perdita, la distruzione o il danno accidentale.

L'uso dei supporti informatici, della posta elettronica, dei programmi informatici, della rete internet deve avvenire conformemente nel rispetto di quanto previsto nelle procedure del Sistema Gestione Qualità, integralmente richiamata per quanto di competenza.

4.1. Documentazione integrativa

La presente procedura richiama ed integra quanto già disciplinato nell'ambito della seguente documentazione:

- Statuto
- Codice Etico
- Poteri deleghe e procure
- Documento per la pianificazione e gestione in materia di prevenzione del malaffare ex L. 190/2012 e trasparenzaMisure Integrative per la prevenzione della corruzione
- Manuale del Sistema di Gestione Integrato per la Qualità e l'Ambiente
- Sistema di Gestione per la Qualità, con particolare - ma non esclusivo - riferimento alla procedura "*Gestione sistemi informativi"*
- Disciplinare Interno ASP – Email e Internet in ufficio
- Altre procedure del presente MOG 231 cui si rinvia, per quanto di competenza, con particolare – ma non esclusivo – riferimento a:
  - procedura 1 (gestione dei rapporti con l'OdV) per quanto attiene i flussi informativi e le segnalazioni verso l'OdV;
  - procedura 5 (gestione dei rapporti di industria e commercio) per quanto attiene il rapporto con le altre imprese;
  - procedura 10 (gestione dei rapporti consulenziali) per quanto attiene la gestione del rapporto con il consulente informatico;
  - procedura 14 (tutela del dipendente che segnala irregolarità e possibili episodi di corruzione (c.d. Whistleblowing) per quanto attiene le segnalazioni all'RPCT;

4.2. Procedure da applicare

Ai fini della prevenzione dei reati di cui al D.lgs. 231/01, occorre segnatamente:

a) gestione delle postazioni informatiche

- catalogare tutte le macchine presenti evidenziando il software caricato, indicando l'eventuale data di scadenza delle singole licenze;
- introdurre protezioni in grado di limitare l'accesso ai siti internet contenenti materiale pedopornografico;
- dotare ogni postazione informatica di password personalizzata abbinata allo username dell'utente, predisponendo la registrazione di ogni accesso;
- dotare ogni postazione informatica abilitata all'accesso ad internet di password personalizzata abbinata allo username dell'utente, predisponendo la registrazione di ogni accesso;

- dotare ogni postazione informatica di meccanismi di stand-by protetti da password abbinata a username, al fine di evitare l'utilizzo indebito della macchina in caso di allontanamento temporaneo dell'utente;
- modificare le password almeno semestralmente; ogni Destinatario è tenuto a custodire la propria password in modo da evitarne la divulgazione.

b) protezione dei sistemi informatici o telematici da eventuali danneggiamenti

A seguito dell'entrata in vigore, in data 5.04.2008, della Legge 18 marzo 2008 n. 48, attuativa della Convenzione del Consiglio d'Europa in tema di criminalità informatica, ai fini della prevenzione dei reati così introdotti ai sensi del D.lgs. 231/2001, in uno con quanto dettato sopra, occorre:

- individuare le persone fisiche abilitate all'accesso al server aziendale;
- individuare le persone fisiche abilitate all'accesso ai sistemi informatici e alle banche dati nel rispetto della normativa in materia di trattamento dei dati personali;
- esplicitare i sistemi informatici e telematici e le relative banche dati accessibili, vietando l'accesso a quelli non espressamente indicati;
- esplicitare i limiti di azione delle persone suddette all'interno dei sistemi telematici e delle banche dati, predisponendo misure tecniche ed organizzative adeguate volte ad attuare in maniera efficace i principi di protezione dei dati;

c) predisposizione o utilizzo di documenti informatici pubblici aventi efficacia probatoria

Nel caso di predisposizione o uso di documenti informatici qualificabili come atto pubblico, copia autentica e/o attestato, occorre:

- verificare la provenienza e la veridicità del documento e del suo contenuto;
- conservare il documento cartaceo e la relativa documentazione cartacea probante la veridicità del suo contenuto e la sua provenienza nel fascicolo di competenza (da costituirsi necessariamente all'atto della predisposizione o dell'utilizzo di un documento informatico di cui sopra qualora esso non faccia parte di un fascicolo già esistente – ad esempio archivio fatture);
- arrestare il procedimento di predisposizione, utilizzo o invio allorquando la provenienza e/o la veridicità del documento o del suo contenuto siano dubbi, nonché informarne senza indugio le competenti autorità aziendali e l'RPCT mediante gli appositi canali previsti nella "Procedura per la tutela del dipendente che segnala irregolarità e possibili episodi di corruzione (c.d. Whistleblowing) (proc. 14). È fatto divieto di proseguire nell'operazione in assenza di autorizzazione dell'AD.

5. Attività dell'ODV

Premessi i generali poteri di iniziativa e controllo, l'OdV ha facoltà di:

- prendere visione di tutti i documenti concernenti la gestione delle postazioni informatiche;

- accedere ai documenti telematici inviati, al fine di verificare la loro coincidenza con gli atti originali cartacei ovvero con i dati sulla base dei quali è stato predisposto il documento telematico;
- verificare la corrispondenza tra i programmi dichiarati come installati sul PC e quelli effettivamente presenti;
- verificare le licenze dei programmi installati sui PC.

L'OdV incontra (se nominato) il Responsabile della Protezione dei Dati (RDP/DPO) almeno una volta all'anno, nonché ogni volta ciò si renda necessario.

In tali incontri, l'OdV è facoltizzato a richiedere tutte le informazioni ritenute necessarie per verificare la corretta applicazione di quanto previsto nella presente procedura.

6. Disposizioni finali

Tutte le funzioni aziendali coinvolte hanno la responsabilità di osservare e far osservare il contenuto della presente procedura.

Fermo quanto previsto dalla procedura di Gestione dei Rapporti con l'OdV (Proc. 1), ciascun Destinatario è tenuto a comunicare/segnalare tempestivamente all' RPCT ogni anomalia/violazione di quanto previsto dalla presente procedura mediante gli appositi canali previsti nella *"Procedura per la tutela del dipendente che segnala irregolarità e possibili episodi di corruzione*" (c.d. Whistleblowing) (proc. 14)

La violazione della presente procedura e dei suoi obblighi di comunicazione e segnalazione costituisce violazione del MOG231 e illecito disciplinare passibile di sanzione ai sensi di legge e del contratto collettivo nazionale di lavoro applicabile.