PROCEDURA 9
GESTIONE DELLE
ATTIVITA' INFORMATICHE

INDICE:

ALLEGATI:

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)
- art. 260 bis D.Lgs. 152/06 commi 6, 7 e 8 – sistema informatico di controllo della tracciabilità dei rifiuti (art. 25 undecies D.Lgs. 231/01)

- art. 648 c.p. – ricettazione (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, in particolare:

- ✓ AD - Datore di Lavoro ex D.lgs. 81/08 - Gestore ambientale - Delegato in materia fiscale - Delegato in materia urbanistica e vincolistica - Trattamento dei dati personali
- ✓ Direttore Generale
- ✓ Assistente di direzione
- ✓ Procuratore – Responsabile della Direzione Amministrazione, Finanza e Controllo di Gestione - delegato ex art. 16 D.Lgs. 81/08 (per la propria direzione)
- ✓ Amministrazione finanza e controllo
- ✓ Procuratore – Responsabile della Direzione Personale, Organizzazione e Sistemi - delegato ex art. 16 D.lgs. 81/08 (per la propria direzione)
- ✓ Personale organizzazione sistemi
- ✓ Personale Organizzazione Sistemi - Sistemi informativi
- ✓ Servizio appalti e Approvvigionamenti
- ✓ Servizio Appalti e Approvvigionamenti - Area Appalti
- ✓ Procuratore - Responsabile Area Approvvigionamenti e Magazzino
- ✓ Servizio appalti e approvvigionamenti – Approvvigionamenti e magazzino
- ✓ Responsabili Amministrativo del Procedimento (RAP)
- ✓ Responsabili Tecnico del Procedimento (RTP)
- ✓ Responsabile Unico del Procedimento (RUP)
- ✓ Procuratore – Responsabile della Direzione Servizio Idrico Integrato - delegato ex art. 16 D.lgs. 81/08 (per la propria direzione)
- ✓ Procuratore – Responsabile della Direzione Igiene Ambientale - delegato ex art. 16 D.lgs. 81/08 (per la propria direzione)
- ✓ Procuratore - Responsabile del Servizio Gestione Calore - delegato ex art. 16 D.lgs. 81/08 (perla propria direzione)
- ✓ Rappresentante della Direzione - Sistemi di Gestione Qualità Ambiente e Sicurezza

- ✓ Medico competente
- ✓ Consulente IT

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:

- gestione e utilizzo dei sistemi informatici e delle informazioni aziendali (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);
- utilizzo della posta elettronica e della rete Internet;
- gestione delle autorizzazioni e delle licenze di programmi software e banche dati.

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, l'ente 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 Integrato Qualità, Ambiente e Sicurezza, integralmente richiamate per quanto di competenza.

Si precisa che API svolge una serie di servizi a favore di DGN (controllata), APE, APER e ASST come da contratti agli atti della Società, cui si rimanda nella loro formulazione attuale e nelle loro eventuali successive modifiche (di cui l'OdV deve essere tempestivamente informato), tra i quali:

- i servizi informatici.

Al fine di consentire un efficace controllo sui rapporti di service, API e DGN (controllata) nonché le società contrattualmente legate da un contratto di service (APE, APER e ASST) adottano MOG231 e Codice Etico speculari, agevolando la confrontabilità e l'omogeneità delle procedure.

Pertanto, nello svolgimento dei servizi informatici prestati a favore della controllata nonché delle società legate da apposito contratto di service, API è tenuta ad osservare la presente procedura, unitamente agli eventuali ulteriori presidi previsti nel MOG 231 di DGN, APE, APER ed ASST.

I rapporti di service tra API e DGN, APE, APER e ASST sono regolati nell'apposita procedura (proc. 13) del presente MOG 231, cui si fa rinvio.

4.1. Documentazione integrativa

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

- Codice Etico
- Poteri deleghe e procure
- Contratti di service
- Sistema Integrato Qualità, Ambiente e Sicurezza, con particolare – ma non esclusivo – riferimento:
  - Procedura Operativa PO.04.3 "*Utilizzo delle infrastrutture informatiche aziendali*"
  - Istruzione tecnica "*Regolamento gestione PEC*"
- 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 verso l'OdV e tra gli OdV della società controllata e delle società contrattualmente legate da un rapporto di service;
  - 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 13 (gestione dei rapporti infragruppo e di service) per quanto attiene i servizi informatici prestati in forza del contratto di service.

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.

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;
- esplicitare i sistemi informati 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;
- segnalare all'OdV le eventuali anomalie che dovessero essere riscontrate nel corso dell'accesso ad un sistema informatico e telematico avvalendosi del Report di cui alla procedura 1 (*Report 2.1.1. Flussi Informativi verso l'OdV*) ovvero in altra forma scritta comunque idonea.

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

Nel caso di predisposizione o uso di documenti informatici integranti 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'OdV a mezzo di apposito report (avvalendosi del *Report 2.9.1 – Segnalazione Presunte Violazioni* ovvero mediante altra forma scritta comunque idonea).

È fatto divieto di proseguire nell'operazione in assenza di autorizzazione del Direttore Generale.

d) tutela del diritto d'autore

- nel caso si ravvisi la necessità di apposito programma non già caricato sulla macchina in uso (previa regolare licenza), inoltrare una richiesta al Responsabile di settore affinché trasmetta la relativa richiesta di acquisto in forma scritta al Servizio Appalti e Approvvigionamenti che provvederà nel rispetto della Procedura di Gestione degli affidamenti di lavori, servizi e forniture (proc. 3) del presente MOG 231;
- aggiornare tempestivamente il catalogo dei sistemi informatici in uso, a seguito di implementazione degli stessi in ragione dell'acquisto di nuovi programmi.

È fatto divieto a ciascun operatore di postazione informatica di scaricare da internet programmi, files od applicazioni, anche se catalogate come "free download".

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.

6. Disposizioni finali

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

Ciascun Destinatario è tenuto a comunicare tempestivamente all'OdV, oltre a quanto espressamente previsto dalla procedura di Gestione dei Rapporti con l'OdV (Proc. 1), ogni presunta violazione di quanto previsto dalla presente procedura a mezzo di apposito report (*Report 2.1.1 – Flussi Informativi verso l'OdV*) ovvero in altra forma scritta comunque idonea.

La violazione della presente procedura e dei suoi obblighi di comunicazione costituisce violazione del MOG 231 e illecito disciplinare passibile di sanzione ai sensi di legge e del contratto collettivo nazionale di lavoro applicabile.