**Residenza Conte Canevaro**

Via Antica Romana 27

16035 ZOAGLI

Tel. 0185259049 fax 0185250034

CF. 83003590102

e-mail info@residenzacanevaro.com

# PROTOCOLLO 9: GESTIONE DELLE ATTIVITÀ INFORMATICHE

INDICE:



## 1. Obiettivi

Il presente protocollo ha l'obiettivo di definire ruoli e responsabilità, nonché dettare procedure 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, il presente protocollo intende prevenire il verificarsi delle fattispecie di reato previste nei seguenti articoli del D.Lgs. 231/01:

- 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)
- reati 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).

Il presente protocollo 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 (Aree a rischio)

Il presente protocollo trova applicazione nei confronti di tutti coloro che, nell'esercizio dell'attività di propria competenza a favore della Fondazione, utilizzano i sistemi informatici e/o telematici della Fondazione (compresi quindi i Consulenti).

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 della Fondazione. Pertanto, i Destinatari del presente protocollo vanno individuati in tutti coloro che utilizzano un personal computer e/o hanno accesso alla posta elettronica e/o utilizzano programmi informatici e/o della Fondazione, anche accedendo ad internet (compresi quindi I Consulenti che operano per conto della Fondazione).

## 3. Processi aziendali coinvolti (Processi a rischio)

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

a) svolgimento processi che richiedono l'utilizzo dello strumento informatico;
b) supporto tecnico IT
c) legale rappresentanza ed esercizio dei poteri di ordinaria e straordinaria amministrazione – esercizio dei poteri di esclusiva competenza del Cda

## 4. Documentazione integrativa

Ogni postazione informatica deve essere gestita nel rispetto della normativa vigente, della normativa in materia di diritto d'autore, copyright e privacy (D.lgs. n. 196/2003 e REG. UE 2016/679), nonché nel rispetto di tutta la normativa nazionale ed internazionale concernente l'utilizzo dei mezzi informatici.

Il presente protocollo richiama ed integra quanto già disciplinato nell'ambito della seguente documentazione:

- Codice Etico
- Statuto e Atto Costitutivo
- Poteri e nomine, deleghe e procure
- "Misure di Sicurezza sul trattamento dei dati" (Sistema GDPR ex Reg. UE 2016/679)
- Altre procedure del presente MOG cui si rinvia, per quanto di competenza, con particolare – ma non esclusivo – riferimento a:
  - protocollo 1 (gestione dei rapporti con l'ODV) per quanto attiene i flussi informativi verso l'ODV;

- protocollo 3 (gestione dei rapporti consulenziali) per quanto attiene la selezione e la gestione del rapporto con il consulente;
- protocollo 5 (anticorruzione e gestione dei rapporti con le PP.AA) per quanto attiene alla gestione dei rapporti con i soggetti pubblici;
- protocollo 6 (Gestione della Tutela dell'ambiente) posto che i reati ambientali di cui D.lgs. 231/2001 (compreso il divieto di abbandono ex D.lgs. n. 152/2006) possono essere potenzialmente commessi mediante strumenti informatici;
- protocollo 11 (gestione dei rapporti di industria e commercio) per quanto attiene il rapporto con le altre imprese;

## 5. Procedure da applicare

Ai fini della prevenzione dei reati di cui al d.lgs. 231/01 con riferimento ai processi aziendali coinvolti e che si ritengono potenziamente a rischio commissione reato di cui al suddetto decreto come da punto 3 del presente protocollo, si delineano le seguenti procedure

*a) Svolgimento processi che richiedono l'utilizzo dello strumento informatico*

*1) 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;

- in caso di PC utilizzati da più utenti, predisporre più account di accesso, personalizzati con distinti username e password;

- modificare le password almeno semestralmente

*2) 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; in particolare:

- indicare specificamente l'attività che deve essere svolta;
- vietare esplicitamente ogni attività estranea all'operatività aziendale;
- evidenziare e vietare quei comportamenti atti ad intergare i reati in materia informatica e telematica;
- attenersi alle regole dettate dal proprietario del sistema telematico e/o della banca dati;

*3) 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

E' fatto divieto di proseguire nell'operazione in assenza di autorizzazione del Presidente del CDA.

<u>È sempre fatto d'obbligo segnalare all'ODV le eventuali anomalie che dovessero essere riscontrate nel corso dell'accesso a sistemi informatici e telematici altrui.</u>

<u>Tale regolamentazione interna deve essere diffusa tra i Destinatari interessati.</u>

*<u>b)</u>* *<u>Supporto tecnico IT</u>*

L'Amministratore di Sistema incaricato dalla Fondazione, unico e solo destinatario delle presente procedura di prevenzione, ha l'obbligo, nell'esercizio della propria attività, di rispettare le disposizioni legislative e codicistiche nazionali, i principi di cui al Codice Etico della Fondazione, e quanto disposto dallo stesso MOG 231 della Fondazione, in ossequio al dettato del protocollo 3.

c) *legale rappresentanza ed esercizio dei poteri di ordinaria e straordinaria amministrazione – esercizio dei poteri di esclusiva competenza del Cda*

Con riferimento alla *"Legale rappresentanza ed poteri di ordinaria e straordinaria amministrazione*" si rimanda integralmente a quanto disposto nello Statuto e nell'Atto Costitutivo della Fondazione.

In ogni caso, il Presidente del Cda e il Cda devono, nell'esercizio dei poteri loro demandati, operare nel rispetto della normativa nazionale e del Codice Etico

## 6. 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;
- prendere visione del registro delle postazioni informatiche condivise;
- accedere ai documenti telematici inviati, al fine di verificare la loro coincidenza con gli eventuali 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

## 7. Disposizioni finali

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

Ciascun Destinatario è tenuto a comunicare all'ODV, oltre a quanto espressamente previsto dal protocollo 1 del presente MOG231 e dal presente protocollo, ogni anomalia rilevabile in relazione a quanto previsto dal presente protocollo.

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

# Stato delle revisioni

| ***Descrizione*** |
| --- |
| Prima emissione |