PROCEDURA 9
GESTIONE DELLE
ATTIVITÀ 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):

- 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).

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

La presente procedura trova applicazione nei confronti di tutti coloro che, nell'esercizio dell'attività di propria competenza a favore dell'ente, utilizzano i sistemi informatici e/o telematici dell'ente.

I reati di cd. "criminalità informatica" (quali quelli in precedenza indicati) prevedono quale presupposto la disponibilità di uno strumento informatico (pc, laptop, tablet, smartphone, etc.) 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:

- legale rappresentanza e poteri di ordinaria amministrazione
- gestione dei rapporti con i soggetti pubblici
- gestione dell'esecuzione degli appalti e dei contratti
- gestione della funzione di Titolare di licenza di pubblica sicurezza
- gestione delle gare d'appalto
- svolgimento dei processi che richiedono l'utilizzo dello strumento informatico
- gestione della salute e sicurezza

4. Documentazione integrativa

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

- Statuto
- Sistema di governance
- Codice Etico
- Contratto di service
- UNI EN ISO 9001:2015 "Sistemi di Gestione della Qualità", con particolare – ma non esclusivo – riferimento alle procedure:
    - PR-GD "*Gestione documentazione e dati"*
- Altre procedure del presente MOG 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 della Proprietà Intellettuale) per quanto attiene la proprietà intellettuale;
- procedura 12 (Gestione delle attività commerciali) per quanto attiene la gestione delle gare e dei contratti e la trasmissione telematica dei documenti di gara;
- procedura 13 (Gestione dei Rapporti Infragruppo e di Service) per quanto attiene i servizi informatici di cui l'ente usufruisce in forza del contratto di service.

5. Protocolli di prevenzione

Si precisa che CVN S.R.L. ha contrattualmente demandato a CSA S.R.L. una serie di servizi, come da contratto allegato agli atti dell'ente, cui si rimanda nella sua formulazione attuale e nelle sue eventuali successive modifiche (di cui l'OdV deve essere tempestivamente informato), tra i quali:

- supporto e la consulenza informatica.

Nello svolgimento dei servizi di cui sopra, CSA S.R.L.:

- opera sulla base dei dati fornitile dalla società, uniformandosi ai dettami legislativi ed alle regole di massima trasparenza previste dal Codice Etico;
- rispettare la speculare procedura 9 (gestione delle attività informatiche) del proprio MOG231, unitamente agli eventuali ulteriori presidi previsti nel presente MOG231.

I rapporti di service tra la società e la CSA S.R.L. sono regolati nell'apposita procedura di gestione dei rapporti di service (proc. 13) del presente MOG 231, cui si fa rinvio.

***

Le attività informatiche devono essere gestite nel rispetto dei principi condivisi mediante l'adozione del Codice Etico, 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.

È vietato alterare in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenire senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, al fine di procurare alla società o ad altri un ingiusto profitto con altrui danno.

L'ente adotta misure tecniche ed organizzative adeguate volte ad attuare in maniera efficace i principi di protezione dei dati, assicurando che:

- il trattamento dei dati personali avvenga in modo lecito, corretto e trasparente,
- la raccolta dei dati personali avvenga per finalità determinate esplicite e legittime,
- la conservazione dei dati personali avvenga 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 avvenga 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,

nel rispetto della normativa di settore.

Nello specifico occorre conformarsi a quanto segue:

a) gestione delle postazioni informatiche

- catalogare tutte le macchine presenti come previsto nella procedura 5 (gestione della proprietà intellettuale);
- 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; se ciò non fosse possibile, predisporre un registro di turnazione, avvalendosi di apposito report (*Report 2.9.1 – Utilizzo Postazione Informatica Condivisa*) ovvero in altra forma ritenuta più idonea, dal quale sia possibile risalire in base alla fascia oraria di utilizzo all'utente che in quel momento aveva accesso alla postazione informatica;
- modificare le password periodicamente, come prevista dalla normativa di settore; 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, 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 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;
- arrestare il procedimento di predisposizione, utilizzo o invio allorquando la provenienza e/o la veridicità del documento o del suo contenuto siano dubbi, nonché informare senza indugio all'AD. L'OdV deve essere informato a mezzo di apposito report (avvalendosi del *Report 2.9.2 – Segnalazione Presunte Violazioni* ovvero mediante altra forma scritta comunque idonea).

È fatto divieto di proseguire nell'operazione in assenza di autorizzazione dell'AD.

6. Disposizioni finali

Tutti i Destinatari 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'OdV ogni anomalia/violazione di quanto previsto dalla presente procedura a mezzo degli appositi canali previsti nella Procedura di Gestione dei Rapporti con l'OdV (proc. 1).

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 CCNL applicabile.