TRANSMARE s.r.l.

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. 25 octies1. – "delitti in materia di strumenti di pagamento diversi dal contante"

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 di Transmare Srl, utilizzano i sistemi informatici e/o telematici di Transmare Srl (compresi quindi i Consulenti e il Medico Competente) o che comunque agiscono e offrono servizi per conto della società mediante strumenti informatici propri (come 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 di Transmare Srl. 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 di Transmare Srl, anche accedendo ad internet (compresi quindi I Consulenti che operano per conto di Transmare Srl in merito alla gestione del Sistema informatico).

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 allo svolgimento dei processi mediante l'utilizzo del sistema informatico
c) Supporto alla gestione della salute e della sicurezza

4. Documentazione integrativa e principi generali

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
- Poteri e nomine, deleghe e procure
- "Misure di Sicurezza sul trattamento dei dati" (Sistema GDPR ex Reg. UE 2016/679)
- Sistema di Gestione Integrato (UNI EN ISO 9001:2015; UNI EN ISO 14001:2015; UNI EN ISO 45001:2018) – procedura n. 7 "controllo della documentazione", nella parte relativa alla documentazione informatica (pag.3)

Ogni postazione informatica, inoltre, deve essere gestita nel rispetto del Sistema di Gestione Integrato, che viene qui integralmente richiamato per quanto di competenza.

Inoltre, ogni attività e operazione svolta dai soggetti destinatari del presente protocollo per mezzo dello strumento informatico e aventi ad oggetto documenti informatici, dovrà essere posta in essere nel pieno rispetto di quanto disposto dal Codice Etico, dal Sistema di Gestione Integrato di tutta la normativa internazionale e nazionale, e di tutte le procedure di prevenzione di cui ai Protocolli di prevenzione del presente Modello 231/2001 inerenti ad attività aventi ad oggetto l'utilizzo dello strumento informatico.

Quanto sopra esposto diventa parte integrante delle procedure di prevenzione di cui al successivo punto 5.

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;

- segnalare all'ODV le eventuali anomalie che dovessero essere riscontrate nel corso dell'accesso ad un sistema informatico e telematico altrui.

Tale regolamentazione interna deve essere diffusa tra i Destinatari interessati.

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 .

L'autorizzazione di uno dei Soggetti Apicali e/o la prosecuzione dell'operazione in assenza di verifica dell'ODV costituisce violazione grave al MOG231.

4) Ciclo attivo e passivo (gestione dei flussi finanziari). Gestione utilizzo carte di credito e strumenti di pagamento diversi dai contanti

Qualora la predisposizione o l'uso del documento informatico abbia ad oggetto l'ultilizzo di carte di credito e/o di strumenti di pagamento diversi dal contanti, i destinatari del presente protocollo di prevenzione, oltre al osservare tutto quanto asserito sia al suddetto paragrafo 4 che al paragrafo 5 (con particolare rifeirmento al punto 3), devono scrupolosamente osservare quanto predisposto nella procedura di prevenzione e) di cui al protocollo di prevenzione n. 2 "Gestione dei flussi finanziari".

In ogni caso, ogni attività e operazione di cui alla presente procedura svolta dai soggetti destinatari del presente protocollo per mezzo dello strumento informatico e aventi ad oggetto documenti informatici, dovrà essere posta in essere nel pieno rispetto di quanto disposto dal Codice Etico, dal Sistema di Gestione Integrato e di tutta la normative internazionale e nazionale.

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.

Tale regolamentazione interna deve essere diffusa tra i Destinatari interessati.

5) Tutela del diritto d'autore

- Ogni postazione informatica deve rispettare le norme in materia di proprietà intellettuale;
- È fatto divieto a ciascun operatore di postazione informatica scaricare da internet programmi, files od applicazioni, anche se catalogate come "free download";
- Transmare Srl, anche per il tramite del Consulente Informatico, deve controllare i mezzi di comunicazione aziendali e i sistemi informatici (filtro dei siti in conferenti, regole *firewall*, controllo dei livelli di traffico, controllo dei procedimenti di *file sharing*).
- è fatto divieto di impiegare beni aziendali per adottare condotte che violino la tutela dei diritti d'autore;
- nei rapporti con i terzi contraenti Transmare Srl deve apporre clausole riferite all'osservanza delle norme in materia di proprietà intellettuale

b) Supporto Supporto tecnico allo svolgimento dei processi mediante l'utilizzo del sistema informatico

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

c) Supporto alla gestione della salute e della Sicurezza

Il Medico Competente, oltre a dover osservare quanto dettato dal Protocollo di prevenzione 7 inerente alla "Gestione della salute e della Sicurezza", con specifico riferimento al paragrafo n. 6 "procedure da applicare", deve altresì rispettare le procedure di prevenzione di cui al presente protocollo al fine di evitare la commissione dei reati di cui al capitolo 1 e per come indicato nel risk assessment nel documento di Parte Speciale.

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

L'ODV ha facoltà di verificare comunque quanto previsto dal presente protocollo.

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
Approvato con delibera del 22 agosto 2024