TERRA di LAVORO
S.P.A. con socio unico

Società soggetta a Controllo e Coordinamento da Parte dell'Ente Provincia di Caserta

Sede Legale ed Uffici Amministrativi: 81100 Caserta, Via Lamberti n. 29Tel. 0823/21.03.90 - Fax.0823/21.29.87 - www.terradilavorospa.com – Email: info@tlspa.it - PEC: tdl@pec.it
Tel. 0823/15.03.996 – Fax: 0823/15.03.991 – Email: controlloimpianti@tlspa.it – PEC: controlloimpiantitlspa@pec.it

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

PROTOCOLLO REATI INFORMATICI

Sommario

1 SCOPO

Il presente protocollo disciplina gli aspetti inerenti la gestione ed il controllo delle attività aziendali che possono portare alla commissione dei reati cosiddetti "informatici", previsti dall'art 24-bis del Dlgs 231/01 e dall'art. 25-novies del Dlgs 231/01, derivanti dall'utilizzo improprio dei sistemi informativi all'interno della società TERRA DI LAVORO SPA.

Inoltre, in osservanza del Decreto Legislativo n.231 dell'8 giugno 2001 e norme collegate in tema di responsabilità amministrativa degli enti, la presente procedura costituisce parte integrante del Modello di Organizzazione, Gestione e Controllo della TERRA DI LAVORO S.p.A.

La procedura assolve, fra le diverse finalità, il compito di agevolare il monitoraggio dell'applicazione del Modello di Organizzazione Gestione e Controllo da parte dell'Organismo di Vigilanza e di prevenire la commissione, da parte dei soggetti indicati all'art 5 c 1 Dlgs 231/01 dei seguenti reati:

Art. 24 bis D.L.gs 231/2001 "Delitti Informatici e trattamento illecito dei dati"

- ✓ Art. 635- bis c.p. "Danneggiamento di informazioni, dati e programmi informatici"
- ✓ Art. 635- quater c.p. "Danneggiamento dei sistemi informatici o telematici"

Art. 25 novies D.L.gs 231/2001 "Reati in materia di diritti d'autore"

- ✓ Art. 171 Bis Violazione dei Diritti d'Autore mediante duplicazione di programmi"

Violazione delle norme in materia di Perimetro di sicurezza nazionale cibernetica (art. 1, comma 11, D.L. 21 settembre 2019, n. 105)

- ✓ Chiunque, allo scopo di ostacolare o condizionare l'espletamento dei procedimenti di cui al comma 2,lettera b), o al comma 6, lettera a), o delle attività ispettive e di vigilanza previste dal comma 6, lettera c), fornisce informazioni, dati o elementi di fatto non rispondenti al vero, rilevanti per la predisposizione o l'aggiornamento degli elenchi di cui al comma 2, lettera b), o ai fini delle comunicazioni di cui al comma 6, lettera a), o per lo svolgimento delle attività ispettive e di vigilanza di cui al comma 6),lettera c) od omette di comunicare entro i termini prescritti i predetti dati, informazioni o elementi di fatto, e' punito con la reclusione da uno a cinque anni e all'ente, responsabile ai sensi del decreto legislativo 8 giugno 2001, n. 231, si applica la sanzione pecuniaria fino a quattrocento quote.

2 CAMPO DI APPLICAZIONE

La presente procedura per i reati relativi ai delitti informatici si applica alle attività operative svolte all'interno di TERRA DI LAVORO SPA che presuppongono l'utilizzo di strumenti informatici sia hardware che software.

3 RIFERIMENTI NORMATIVI

- D.Lgs 196/2003
- Regolamento Europeo n. 2016/679
- Art. 24-bis, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 48/2008; modificato da D.Lgs. n. 7 e 8/2016 e dal D.L. n. 105/2019 convertito in Legge n. 18.11.2019 n.133]

4 LE FATTISPECIE DI REATO

Documenti informatici (art. 491-bis c.p.)

Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti gli atti pubblici.

Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.)

Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.

La pena è della reclusione da uno a cinque anni:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri, o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;
3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.

Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.

Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.)

Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino a un anno e con la multa sino a cinquemilacentosessantaquattro euro.

La pena è della reclusione da uno a due anni e della multa da cinquemilacentosessantaquattro euro a diecimilatrecentoventinove euro se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617quater.

Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico (art. 615-quinquies c.p.)

Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329..

Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.)

Chiunque fraudolentemente intercetta comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a

quattro anni. Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma. I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa.

Tuttavia, si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso:

1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;

2) da un pubblico ufficiale o da un incaricato di un pubblico servizio con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;

3) da chi esercita anche abusivamente la professione di investigatore privato.

Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.)

Chiunque, fuori dei casi consentiti dalla legge, installa apparecchiature atte a intercettare, impedire o interrompere comunicazioni relative a un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni.

La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617quater

Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.)

Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni. Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni.

Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter c.p.)

Salvo che il fatto costituisca piu‘ grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni. Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l’alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni. Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata.

Danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.)

Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all’articolo 635 bis, ovvero attraverso l’introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni. Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata.

Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.)

Se il fatto di cui all’articolo 635 quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni. Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da

tre a otto anni. Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata.

Frode informatica del certificatore di firma elettronica (art. 640-quinquies c.p.)

Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, è punito con la reclusione fino a tre anni e con la multa da 51 a 1.032 euro.

5 DEFINIZIONI

RPRIV = Responsabile Privacy

Danneggiamento (*vedi art. 635 del Codice Penale***)**: Chiunque distrugge, disperde, deteriora o rende, in tutto o in parte, inservibili cose mobili o immobili;

Trattamento: qualunque Operazione o complesso di operazioni concernenti un utilizzo qualsiasi (raccolta, registrazione, conservazione, distruzione etc.) di dati, anche se non registrati in Banca Dati;

Dato Personale: Qualunque informazione, diretta o indiretta, relativa a persona, fisica o giuridica;

Dato Identificativo: i dati personali che permettono l'identificazione diretta dell'interessato;

Banca Dati: Complesso organizzato di dati ripartito in uno o più unità dislocate in uno o più siti;

Reti di comunicazione elettronica: i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;

Rete pubblica di comunicazioni: una rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico;

Servizio di comunicazione elettronica: i servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, nei limiti previsti dall'articolo 2, lettera c), della direttiva 2002/21/CE del 7 marzo 2002, del Parlamento europeo e del Consiglio;

Posta elettronica: messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza;

Misure minime: il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti dal Regolamento Europeo 2016/679 e d.lgs.196/2003;

Strumenti elettronici: gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;

Autenticazione informatica: l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;

Credenziali di autenticazione: i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;

Parola chiave: componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;

Profilo di autorizzazione: l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;

Sistema di autorizzazione: l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

6 RESPONSABILITA'

Il presente paragrafo intende correlare, per ciascuna funzione aziendale (Responsabile di Servizio, Responsabile di Unità), lo svolgimento delle attività operative ai possibili reati derivanti da Delitti informatici o dal trattamento illecito dei dati e della violazione dei diritti d'autore previsti dal Dlgs 231/01.

Reati **Attività**	Art. 635- bis c.p. "Danneggiamento di informazioni, dati e programmi informatici"	Art. 635- quater c.p. "Danneggiamento dei sistemi informatici o telematici"	Art. 171 Bis Violazione dei Diritti d'Autore mediante duplicazione di programmi"
Gestione del sistema informativo aziendale comprensivo di hardware, software e gestione della rete	Tutti	Tutti	Tutti

7 CLASSIFICAZIONE DEI RISCHI DI COMMISSIONE DEL REATO

La sottostante tabella riporta l'esito della classificazione del rischio di commissione del reato descritta nel Modello di Organizzazione, Gestione e Controllo per i soggetti responsabili indicati nel paragrafo precedente

Classificazione del rischio **Reati**	Molto Basso	Basso	Medio	Alto	Molto Alto
Art. 635- bis c.p. "Danneggiamento di informazioni, dati e programmi informatici"		**X**			
Art. 635- quater c.p. "Danneggiamento dei sistemi informatici o telematici"		**X**			
Art. 171 Bis Violazione dei Diritti d'Autore mediante duplicazione di programmi"		**X**			

8 MODALITA' OPERATIVE

8.1 PRINCIPI GENERALI DI COMPORTAMENTO

Uno dei presupposti del Modello al fine i reati "informatici" è dato dal rispetto di alcuni principi e nella tenuta di determinati comportamenti, da parte dei lavoratori della Società, nonché dagli eventuali soggetti esterni che siano coinvolti nelle attività operative che possono esporre la TERRA DI LAVORO SPA al reato presupposto.

TERRA DI LAVORO SPA promuove l'utilizzo della rete e dei supporti elettronici quale strumento utile per perseguire le proprie finalità.

Gli utilizzatori di strumenti elettronici e informatici manifestano liberamente il proprio pensiero nel rispetto dei diritti degli altri utenti e di terzi, nel rispetto dell'integrità dei sistemi e delle relative risorse fisiche, in osservanza delle leggi, norme e obblighi contrattuali.

Consapevoli delle potenzialità offerte dagli strumenti informatici e telematici, gli utenti si impegnano ad agire con responsabilità e a non commettere abusi aderendo a un principio di autodisciplina.

Il posto di lavoro costituito da personal computer viene consegnato completo di quanto necessario per svolgere le proprie funzioni, pertanto è vietato modificarne la configurazione.

Il software installato sui personal computer è quello richiesto dalle specifiche attività lavorative dell'operatore. È pertanto proibito installare qualsiasi programma da parte dell'utente o di altri operatori, escluso l'amministratore del sistema.

I dati di tutte le Postazioni elettroniche e quelle relative al personale che può accedere viene conservato dal responsabile del Sistema Informativo.

La TERRA DI LAVORO SPA al fine di prevenire ogni possibile utilizzo non consentito degli strumenti elettronici e della rete aziendale ha adottato le misure minime previste dall'Allegato B del D.l.gs 196/2003 in materia di tutela e trattamento dei dati.

8.2 ATTIVITÀ SENSIBILI NELL'AMBITO DEI REATI INFORMATICI

Attraverso un'attività di mappatura delle aree a rischio e di controllo, la Società ha individuato le attività sensibili di seguito elencate, nell'ambito delle quali, potenzialmente, potrebbero essere commessi alcuni dei reati informatici o i reati relativi ai diritti d'autore:

a. Installazione di apparecchiature per il danneggiamento dei dati contenuti nel sistema informativo aziendale;
b. Danneggiamento volontario di sistemi informatici o telematici.

Va subito sottolineato come la realizzazione dei delitti informatici è di natura dolosa, quindi una violazione volontaria dei soggetti, rispetto ai protocolli operativi.

8.3 PROTOCOLLI DI PREVENZIONE

Si elencano le misure minime atte a garantire l'integrità e la disponibilità dei dati:

- Le protezioni delle aree e dei locali
- La custodia e l'archiviazione di atti, documenti e supporti
- Le misure logiche di sicurezza
- I criteri di ripristino dei dati

8.3.1 Protocolli specifici di prevenzione

Di seguito sono riportati i protocolli specifici di prevenzione nell'ambito di ciascuna area sensibile a rischio reato identificata e valutata attraverso l'analisi dei rischi allegata al modello organizzativo effettuato dalla TERRA DI LAVORO SPA.

a. Installazione di apparecchiature per il danneggiamento dei dati contenuti nel sistema informativo aziendale.

Gli strumenti elettronici sono affidati ad ogni dipendente all'interno di TERRA DI LAVORO SPA

Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare i reati presupposto esplicitamente richiamati dalla presente procedura.

Come già detto in precedenza, per evitare l'utilizzo di postazioni informatiche e di accessi alla rete è

proceduralizzata una gestione delle Password e delle postazioni.

b. Danneggiamento volontario di sistemi informatici o telematici.

Le regola e i protocolli indicati in precedenza per l'attività a) sono riportabili in modo identico anche per la prevenzione di eventuali danneggiamenti del sistema informatico e telematico.

8.4 CONTROLLO OPERATIVO

L'azienda Istituisce ed attua un sistema di monitoraggio di 1° livello al fine di determinare in controllo strategico degli adempimenti in materia di sicurezza delle informazioni e la tutela delle norme in materia di Privacy.

Tale sistema di monitoraggio prevede l'applicazione:

1. Con periodicità annuale il responsabile delle privacy procede alla verifica sul posto di lavoro dell'applicazione delle misure in materia di trattamento dati.

9 FLUSSO INFORMATIVO ALL'ORGANISMO DI VIGILANZA

Da	Oggetto	Periodicità
RPRIV	Incidenti durante la procedura di incidente e ripristino.	Al verificarsi dell'evento o annualmente anche in assenza di eventi
RPRIV	Attacchi da parte di virus o altre minacce al sistema informatico	Al verificarsi dell'evento o annualmente anche in assenza di eventi
RPRIV	Relazione annuale sull'andamento dei controlli e sul funzionamento del sistema informativo	Annuale
RPRIV	Anomalie relative al: - back up dei dati; - sistema di sicurezza logica e fisica del sistema informativo; - gestione degli strumenti informatici; - danneggiamento o rimozione di software in service per la gestione delle attività; - danneggiamento o rimozione di hardware in service per la gestione delle attività; - uso della rete locale e remota.	Al verificarsi dell'evento o annualmente