ALMALAUREA srl

PARTE SPECIALE DEL MODELLO DI ORGANIZZAZIONE E GESTIONE

REATI INFORMATICI E TRATTAMENTO ILLECITO DEI DATI

Predisposto da Studio Avv. Stefano Termanini
Adottato nella seduta del 23 luglio 2021 del Consiglio di Amministrazione
Pubblicato sul sito internet nella sezione “Amministrazione trasparente”

Sommario

1. Introduzione

In data 5 aprile 2008 è entrata in vigore la Legge n. 48, recante la ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica.

Con tale norma il Legislatore ha apportato modifiche al codice penale in materia di reati informatici ed ha introdotto al D. Lgs. 231/01, l'art. 24 bis per la punibilità dell'Ente in relazione ai delitti informatici e al trattamento illecito dei dati.

I delitti oggetto di tale parte speciale sono puniti con sanzione pecuniaria da 100 a 500 quote, ad esclusione degli illeciti previsti dagli artt. 615-quater e 615-quinquies C.P. e dagli artt. 491-bis e 640-quinquies C.P. per i quali il D. Lgs. 231/01 prevede sanzioni pecuniarie pari a 300 quote per i primi e 400 quote per i restanti.

In caso di violazione delle disposizioni di cui all'art. 24 bis del citato decreto, potranno vedersi altresì applicate le sanzioni pecuniarie di cui all'art. dall'articolo 9, comma 2 D. Lgs. 231/01.

2. I reati e le possibili modalità di commissione

Accesso abusivo ad un sistema informatico o telematico (art. 615-*ter* C.P.)

L'articolo citato punisce l'introduzione abusiva in un sistema informatico o telematico protetto da misure di sicurezza ovvero la permanenza all'interno del sistema contro la volontà espressa o tacita di chi ha il diritto di esclusione.

La fattispecie di reato è da considerarsi integrata anche quando il soggetto agente è autorizzato ad accedere al sistema informatico ma vi accede violando i limiti risultanti dalle prescrizioni impartite dal titolare del sistema o attuando operazioni diverse rispetto a quelli per le quali è autorizzato ad accedere al sistema.

Il suddetto reato può concorrere con il reato di cui all'art. 640-*ter* C.P. (frode informatica) trattandosi di fattispecie che tutelano diversi beni giuridici.

Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-*quater* C.P.)

Tale ipotesi criminosa punisce 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 già menzionato scopo.

Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-*quinquies* C.P.)

Il reato in oggetto punisce 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"

Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (617-*quater* C.P.)

La fattispecie punisce chiunque intercetti fraudolentemente comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero impedisca o interrompa il regolare svolgimento di tali comunicazioni. La stessa disposizione punisce altresì chi delle citate comunicazioni rivela il contenuto mediante qualsiasi mezzo di informazione al pubblico.

Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (617-*quinquies* C.P.)

Tale ipotesi di reato punisce l'installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, salvi i casi previsti dalla legge.

Danneggiamento di informazioni, dati e programmi informatici (art. 635-*bis* C.P.)

L'ente è punibile anche in caso di reati relativi a distruzione, deterioramento, cancellazione, alterazione o soppressione di informazioni, dati o programmi informatici altrui.

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

Responsabilità dell'Ente anche in tale ipotesi di reato che si configura in relazione a fatti diretti 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.

Danneggiamento di sistemi informatici o telematici (art. 635-*quater* C.P.)

L'ipotesi di reato si configura nel caso in cui, mediante le condotte di cui all'articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, vi sia distruzione, danneggiamento o inservibilità, in tutto o in parte, di sistemi informatici o telematici altrui ovvero qualora il funzionamento degli stessi venga gravemente ostacolato.

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.

Frode informatica (art. 640-*ter* C.P., richiamato da art 24 D. Lgs. 231/01)

Tale ipotesi di reato si configura nel caso in cui, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, il soggetto agente procuri a sé o ad altri un ingiusto profitto con altrui danno.

A titolo meramente esemplificativo, tale condotta può concretizzarsi nelle pratiche di concorrenza sleale volte all'ottenimento di informazioni altrui, ovvero mediante pratiche di *phishing*.

A partire dal 16.10.2013 con l'entrata in vigore della legge di conversione n. 119/2013 del d.l. n. 93/2013 è stato inserito nell'art. 640-ter il terzo comma che prevede la pena della reclusione da due a sei anni e della multa da euro 600 a euro 3.000 se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti.

Si rileva come il reato di frode informatica si differenzi dal reato di danneggiamento di dati informatici in ragione del fatto che nella prima ipotesi delittuosi il sistema informatico continua a funzionare, benché in modo alterato rispetto a quanto programmato, nella seconda ipotesi lo stesso funzionamento risulta minato.

Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-*quinquies* C.P.)

Il reato è previsto in caso di prestazione di servizi di certificazione di firma elettronica, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, con violazione degli obblighi previsti dalla legge per il rilascio di un certificato qualificato.

Delitti di falso riferiti ai documenti informatici aventi efficacia probatoria(art. 491 bis C.P.)

Si tratta dei delitti previsti dal Capo III, Titolo VII, Libro II C.P., concernente i delitti di falso materiale o ideologico.

3. Destinatari e struttura aziendale esistente

La presente parte speciale è diretta a tutti gli esponenti aziendali, tanto a coloro che svolgono la propria attività lavorativa utilizzando strumenti informatici, quanto a coloro che svolgono mansioni per le quali non è necessario utilizzare strumenti informatici.

Maggiormente esposti al rischio di commissione dei reati di cui in parola saranno coloro che per ragioni inerenti alla propria attività lavorativa, si avvalgono regolarmente di strumenti informatici.

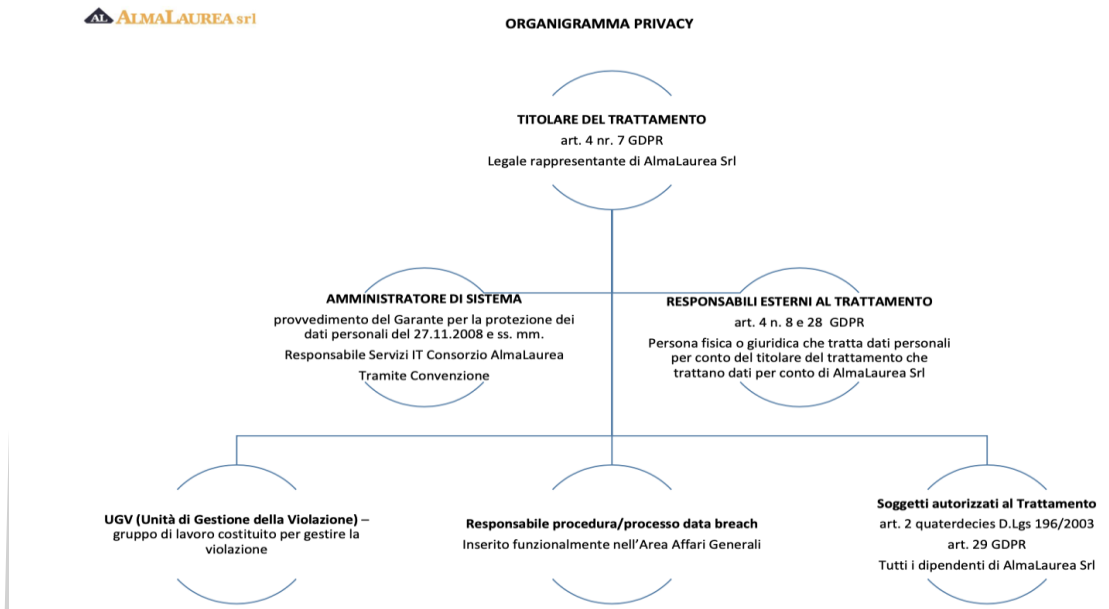
Sul punto, AlmaLaurea S.r.l. è dotata dei seguenti documenti, rilevanti rispetto alla gestione della privacy in azienda, ma anche, in senso trasversale, rispetto alla gestione in via generale della sicurezza informatica:

A. documento contenente le MISURE DI SICUREZZA in materia di gestione dei dati e di gestione della privacy;

B. procedura specifica per la gestione dei fenomeni di DATA BREACH (ex GDPR);

C. disciplinare relativo all'utilizzo dei dati;

D. specifico organigramma di gestione della riservatezza dei dati, che si riporta a seguire.



AlmaLaurea S.r.l. si è anche dotata, nel corso dell'anno 2021, di apposita polizza assicurativa contro il rischio informatico.

Si specifica, infine, che la gestione della materia informatica viene attuata, all'interno di AlmaLaurea S.r.l., in collaborazione ed in affidamento al Socio unico Consorzio Interuniversitario AlmaLaurea, per il tramite di apposita convenzione.

4. Aree di rischio

I reati sopra descritti presuppongono l'utilizzo di strumenti informatici, nonché l'abuso di tali strumenti nell'interesse o a vantaggio della Società.

In generale, vengono definite aree a rischio, tutte quelle aree aziendali che, per lo svolgimento della propria attività, fanno uso di strumenti informatici, con particolare riferimento alle sub-aree preposte al controllo degli strumenti informatici ed al regolare funzionamento degli stessi, nonché a quelle che potrebbero accedere, quantomeno in linea teorica, agli strumenti informatici altrui.

Il rischio è ipotizzabile per tutti i cicli aziendali, stante l'utilizzo quotidiano da parte di tutti i dipendenti di strumenti informatici, posto che talune fattispecie di reato si perfezionano mediante

l'accesso abusivo ad un sistema informatico o telematico da parte di chi non sia autorizzato, oppure mediante il reperimento abusivo, la riproduzione, la diffusione, la comunicazione o la consegna di codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza.

Si rileva altresì come la società disponga di un sistema VPN per accesso remoto ai server, i quali sono protetti da firewall. I dipendenti hanno la possibilità di consultare il database aziendale limitatamente alle cartelle per le quali la dirigenza ha fornito loro apposita password ed ID, in questo modo si consente altresì l'identificazione dell'utilizzatore di ciascun terminale.

Soggetti esterni (soprattutto clienti, ma anche tecnici, installatori, etc.) possono accedere alla strumentazione IT solo ed esclusivamente sotto il controllo del preposto designato dall'Organo Amministrativo solo quando ve ne è la necessità e, in osservanza alle MISURE DI SICUREZZA esistenti, solo previa contrattualizzazione del rapporto. I soggetti esterni accedono attraverso password specifica ed utenza specifica legata alla mail personale fornita al momento di conclusione del contratto. I dati a cui hanno accesso i soggetti esterni – clienti – sono accessibili da parte dei medesimi attraverso la creazione di appositi "ambienti" ad hoc, che contengono solamente i dati relativi al singolo progetto o, comunque, oggetto di specifica condivisione. Ogni utenza, inoltre, è personale e specifica.

I dati sono conservati e categorizzati secondo livelli di riservatezza legati agli specifici ruoli ed alle specifiche funzioni dei singoli operatori. Tutte le cartelle sono clusterizzate in base al ruolo ed alle funzioni dei singoli.

Le aree di attività ritenute più specificamente a rischio individuate sono le seguenti:

1. utilizzo della rete aziendale, del servizio di posta elettronica e di accesso ad Internet;
2. gestione della rete informatica aziendale, evoluzione della piattaforma tecnologica e applicativa IT nonché sicurezza informatica;
3. erogazione di servizi di accesso ai dati nei confronti di terzi;
4. trasmissione di documenti in formato elettronico alla PA nei casi di partecipazione a bandi per l'erogazione di contributi e/o finanziamenti;
5. effettuazione di accessi presso la rete aziendale di terzi;
6. affidamento del servizio di gestione, manutenzione, controllo, o comunque consenso all'accesso alla rete aziendale a terzi, partner, soci.

Le aree a rischio reato, così identificate, costituiscono il punto di riferimento nella definizione delle procedure di controllo.

5. Principi generali di comportamento

La presente parte speciale si riferisce a comportamenti posti in essere da amministratori, dirigenti e dipendenti operanti nelle aree di attività a rischio, nonché da collaboratori esterni e *partners*: tali soggetti vengono definiti, nel loro insieme, Destinatari.

Obiettivo della presente parte speciale è di fare in modo che tutti i Destinatari, nella misura in cui sono coinvolti nello svolgimento di attività nelle aree a rischio, si attengano a regole di condotta conformi a quanto prescritto, dalla parte speciale stessa, al fine di prevenire ed impedire il verificarsi dei reati sopracitati.

La presente parte speciale ha la funzione di:

A) fornire i principi generali e procedurali specifici cui i Destinatari, in relazione al tipo di rapporto in essere con l'impresa, sono tenuti ad attenersi per una corretta applicazione del Modello;

B) fornire all'OdV e ai responsabili delle altre funzioni aziendali, chiamati a cooperare con lo stesso, gli strumenti operativi per esercitare le attività di controllo, monitoraggio e verifica previste.

Principi generali di comportamento

Nell'espletamento di tutte le operazioni attinenti alla gestione sociale, oltre alle regole di cui al presente Modello, i Destinatari devono, in generale, conoscere e rispettare, con riferimento alla rispettiva attività, le regole ed i principi contenuti nei seguenti documenti: il codice etico, le disposizioni organizzative interne (procure e deleghe, *job description*, livelli di approvazione, *flow charts*, linee guida, procedure interne, ecc.) per la parte che regolamenta lo svolgimento delle attività a rischio sopra individuate ed ogni altra normativa relativa al sistema di controllo interno in essere.

Ai collaboratori esterni, laddove esistenti, deve essere resa nota l'adozione del Modello e del codice etico: il rispetto dei principi contenuti in tali documenti costituisce obbligo contrattuale a carico di tali soggetti.

La presente parte speciale prevede l'espresso divieto, a carico degli esponenti aziendali, in via diretta, ed a carico dei collaboratori esterni, di:

1. attuare comportamenti tali, da integrare le fattispecie di reato considerate dell'art. 24-*bis* del D. Lgs. 231/2001;

2. realizzare comportamenti che, sebbene non risultino tali da costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarle;

3. contribuire a configurare situazioni di conflitto di interessi in relazione a quanto previsto dalle già menzionate ipotesi di reato.

Nell'espletamento di tutte le operazioni, oltre alle regole di cui al presente Modello, i Destinatari devono, in generale, conoscere e rispettare, con riferimento alla rispettiva attività, le regole ed i principi contenuti nel Codice Etico e in tutti i documenti aziendali atti a regolare tali attività. A titolo esemplificativo, ma non esaustivo:

- il disciplinare aziendale sulla sicurezza informatica e GDPR;

- la parte generale e la presente parte speciale del presente Modello;

- ogni altro documento/procedura instaurata relativamente al trattamento dei dati tramite supporti informatici;

- ogni altra normativa relativa al sistema di controllo interno in essere;

- tutte le procedure esistenti in azienda, nonché le disposizioni di matrice contrattuale che disciplinano i limiti di accesso alla rete aziendale.

Nell'ambito dei suddetti comportamenti, è fatto divieto in particolare di:

a) effettuare accessi e qualsiasi operazione ai sistemi informatici altrui e ai dati altrui con ciò intuendosi anche alla posta certificata altrui, all'indirizzo di posta elettronica altrui, anche dei colleghi, se non autorizzata da apposito accordo contrattuale e comunque con violazione delle procedure esistenti in materia di trattamento dei dati personali (Regolamento generale sulla protezione dei dati n. 2016/679);

b) utilizzare i sistemi informatici della Società per finalità non connesse alla mansione svolta o comunque contrarie al Codice Etico e ai principi inclusi nel presente Modello;

c) alterare documenti informatici, pubblici o privati, aventi efficacia probatoria;

d) accedere abusivamente al proprio o all'altrui sistema informatico o telematico al fine di alterare e/o cancellare dati e /o informazioni;

e) detenere e utilizzare abusivamente codici, parole chiave, o altri mezzi idonei all'accesso a un sistema informatico o telematico altrui;

f) svolgere attività fraudolenta di intercettazione, impedimento o interruzione di comunicazioni relative a un sistema informatico o telematico di soggetti, pubblici o privati, al fine di acquisire informazioni riservate;

g) installare apparecchiature per l'intercettazione, impedimento o interruzione di comunicazioni di soggetti pubblici o privati;

h) svolgere attività di modifica e/o cancellazione di dati, informazioni o programmi di soggetti privati o soggetti pubblici o comunque di pubblica utilità.

Fermo restando quanto precede, appare utile riportare i principi generali di azione.

Principi generali:

- disponibilità dei dati, ossia salvaguardia del patrimonio informativo nella garanzia di accesso, usabilità e confidenzialità dei dati con l'obiettivo di ridurre a livelli accettabili i rischi connessi all'accesso alle informazioni (intrusioni, furto di dati, ecc.);

- integrità dei dati, ossia il principio volto a garantire che l'informazione non subisca modifiche o cancellazioni a seguito di errori o di azioni volontarie, ma anche a seguito di malfunzionamenti o danni dei sistemi tecnologici;

- riservatezza informatica, intesa come gestione della sicurezza in modo tale da mitigare i rischi connessi all'accesso o all'uso delle informazioni in forma non autorizzata.

Principi procedurali specifici

AlmaLaurea S.r.l. si è dotata di apposite procedure volte ad attuare i principi legislativi in materia di gestione dei sistemi informatici ed in materia di tutela della riservatezza dei dati personali.

Particolare attenzione, in questo frangente, deve essere riservata al documento riportante le MISURE DI SICUREZZA adottate in azienda ai sensi dell'art. 32 del GDPR, trattandosi di schemi procedurali atti a consentire la gestione corretta dell'aspetto informatico generale aziendale.

Nello specifico, si richiamano in questa sede le diverse tipologie di misure adottate:

- misure specifiche;

- misure generali di sicurezza fisica e logica;

- misure organizzative e processi di governo.

Tra le **misure specifiche**, pare utile segnalare, in quanto trasversali:

- cifratura dei dati;

- pseudonimizzazione dei dati;

- controllo degli accessi logici ed autenticazione, che avviene secondo ruoli e responsabilità ben definite e secondo il criterio della c.d. minima conoscenza, secondo cui ogni utente ha accesso ai dati strettamente necessari per lo svolgimento delle proprie mansioni.

Tra le **misure generali**, pare invece utile richiamare:

- sicurezza dell'ambiente operativo (relative alla gestione della sicurezza dei server e del database);

- sicurezza della rete e delle comunicazioni (es. firewall, sonde di rilevamento intrusione, altri dispositivi attivi o passivi di sicurezza della rete);

- tracciatura e monitoraggio delle operazioni compiute dagli utenti sulla rete;

- gestione sicura della postazione di lavoro (relativa alle procedure in essere per evitare che determinate operazioni degli utenti possano mettere a rischio la sicurezza informatica. Ad esempio, costituiscono operazioni vietate la disattivazione del sistema antivirus e l'installazione di software non autorizzati).

Tra le **misure organizzative/principi di governo**, infine, meritano di essere richiamate le seguenti:

- esistenza di un modello organizzativo e di gestione dei dati personali transitanti sulla rete aziendale, il quale individua ruoli e responsabilità di chi ha accesso ai citati dati secondo il principio del c.d. minimo privilegio;

- gestione dei rapporti con le terze parti che, a qualsiasi titolo, gestiscano dati per conto di AlmaLaurea S.r.l. improntata al principio di formalizzazione. In altri termini, la gestione dei dati ad opera di terzi deve sempre essere oggetto di apposito accordo contrattuale;

- esistenza di una specifica procedura per i fenomeni di data breach;

- formazione del personale sulle tematiche connesse alla gestione dei dati personali ed alla sicurezza informatica.

La gestione della sicurezza informatica in azienda avviene nel rispetto dei seguenti standard:

- la **chiara attribuzione di compiti e responsabilità** in materia informatica, secondo il principio di segregazione delle funzioni che vige per tutti gli ambiti di attività e che comporta la riconducibilità, in capo a singoli soggetti, delle azioni compiute;

- la predisposizione e mantenimento del **censimento degli strumenti informatici** in uso alla Società; detto inventario deve riguardare sia l'hardware che il software che le applicazioni in uso;

- la previsione di **periodiche e regolari analisi del rischio** al fine di identificare eventuali punti deboli nel sistema di sicurezza aziendale, stabilire le priorità e formulare un piano di azione la cui attuazione dovrà essere valutata nell'ambito della successiva analisi del rischio;

- la regolamentazione del **corretto utilizzo degli strumenti informatici da parte degli utenti**, fornendo apposita formazione, anche attraverso la creazione e l'implementazione di apposita procedura aziendale.

- l'adozione di **sistema antivirus** sia in entrata che in uscita;

- l'effettuazione di regolari e frequenti **back-up** dei dati aziendali;

- la definizione di un **sistema di emergenza**, ovvero predisposizione di tutte le procedure tecnico/organizzative per poter affrontare stati di emergenza e garantire la *business continuity* attraverso meccanismi di superamento di situazioni anomale;

- l'attuazione di una politica di **formazione e/o di comunicazione** inerente alla sicurezza informatica volta a sensibilizzare tutti gli utenti;

- la previsione di immediata segnalazione da parte di tutti gli utenti al soggetto previamente individuato come incaricato della gestione delle **procedure di Data Breach**, di eventuali incidenti relativi alla sicurezza dei dati.

Ad ogni buon conto ed a prescindere da quanto precede, si elencano di seguito le **regole** che devono essere rispettate dai Destinatari della presente parte speciale:

1. è vietato installare, negli apparecchi in dotazione, programmi software di alcun tipo, se non espressamente autorizzati dal responsabile IT;

2. non è consentito l'uso di programmi e software non distribuiti ufficialmente dal responsabile IT;

3. è vietato modificare le configurazioni impostate sul PC concesso in uso dall'impresa;

4. è vietata l'installazione sul PC in uso o comunque su strumenti informatici dell'azienda, di mezzi di comunicazione propri;

5. i dati riferiti a terze parti devono essere gestiti come riservati;

6. è vietato ottenere credenziali di accesso a sistemi informatici o telematici aziendali di AlmaLaurea S.r.l., dei clienti o di terze parti, con metodi o procedure differenti da quelle per tali scopi autorizzate dalla Società;

7. è vietato attuare, direttamente o ricorrendo a soggetti terzi, comportamenti come il phishing, l'hacking o la diffusione di programmi di malware finalizzati al furto e/o all'indebito utilizzo dell'identità digitale;

8. è vietato divulgare, cedere o condividere con personale interno o esterno alla Società le proprie credenziali di accesso ai sistemi e alla rete aziendale;

9. è vietato accedere ad un sistema informatico altrui (anche di un collega), nonché manomettere ed alterarne i dati ivi contenuti;

10. è vietato manomettere, sottrarre o distruggere il patrimonio informatico aziendale della società, di clienti o di terze parti, comprensivo di archivi, dati e programmi;

11. è vietato effettuare prove o tentare di compromettere i controlli di sicurezza di sistemi informatici aziendali, a meno che non sia esplicitamente previsto nei propri compiti lavorativi;

12. è vietato effettuare prove o tentare di compromettere i controlli di sicurezza di sistemi informatici o telematici di clienti o terze parti a meno che non sia esplicitamente richiesto e autorizzato da specifici contratti o previsto nei propri compiti lavorativi;

13. è vietato sfruttare eventuali vulnerabilità o inadeguatezze nelle misure di sicurezza dei sistemi informatici o telematici, di clienti o di terze parti, per ottenere l'accesso a risorse o informazioni diverse da quelle cui si è autorizzati ad accedere, anche nel caso in cui tale intrusione non provochi un danneggiamento a dati, programmi o sistemi;

14. è vietato comunicare a persone non autorizzate, interne o esterne alla Società, i controlli implementati sui sistemi informativi e le modalità con cui sono utilizzati;

15. è proibito distorcere, oscurare sostituire la propria identità e inviare e-mail riportanti false generalità o contenenti virus o altri programmi in grado di danneggiare o intercettare dati.

* * *