8. PROTOCOLLO PER LA GESTIONE DEI SISTEMI INFORMATICI E TUTELA DEI DIRITTI D'AUTORE

Sommario

1. Principi generali

Al fine di prevenire i reati presupposto informatici, tutti i soggetti che a qualunque titolo accedono e utilizzano i sistemi informatici aziendali devono rigorosamente attenersi alle disposizioni societarie adottate e quelle contenute nel presente Protocollo.

Ci si deve attenere a quanto previsto nel presente Protocollo anche al fine di prevenire i reati in materia di violazione del diritto d'autore.

Tutti i soggetti coinvolti nel processo devono rispettare quanto dettato dalle normative vigenti e applicabili alla Società in materia; la Società deve porre in essere tutti gli investimenti richiesti per operare secondo norma in modo da non generare un indebito risparmio di spesa, poi riutilizzabile nelle attività aziendali.

È fatto divieto a tutti i dipendenti di:

- utilizzare le apparecchiature informatiche aziendali per motivi personali e/o per visualizzare, detenere, inviare commercializzare materiali osceni, istiganti all'odio, discriminatori o molesti;
- utilizzare le apparecchiature informatiche di altri dipendenti senza autorizzazione o utilizzare password di altri utenti aziendali;
- lasciare incustodito o accessibile a terzi il proprio personal computer;
- utilizzare apparecchiature informatiche private, connettendole in qualsiasi modo alla rete informatica della Società;
- installare sul computer o sui dispositivi della Società, assegnati dispositivi di memorizzazione, comunicazione o altro (masterizzatori, modem, chiavi USB) senza la preventiva autorizzazione del Direttore;
- duplicare ogni altro supporto multimediale atto a contenere dati di qualsiasi natura protetti dalla normativa a tutela del diritto d'autore;
- utilizzare opere dell'ingegno protette da diritto d'autore (ad es. programmi per elaboratore, banche dati) in assenza di specifica autorizzazione dell'avente diritto o del pagamento dei relativi diritti
- alterare, contraffare, distruggere documenti informatici (es. scritture private, contratti, dichiarazioni certificati o autorizzazioni amministrative) aventi efficacia probatoria;
- accedere abusivamente (anche con psw/codici di autenticazione di altri) al sistema informatico o telematico di soggetti pubblici o privati;
- detenere, diffondere e/o utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso ad sistema informatico o telematico di terzi, al fine di acquisire informazioni riservate o alterare, cancellare dati e/o informazioni;
- diffondere, tramite posta elettronica o supporti rimovibili, all'interno di sistemi informatici appartenenti a terzi (sia pubblici che privati) virus che possano danneggiare il sistema informatico, le informazioni, i

dati o i programmi in esso contenuti ovvero che ne favoriscano l'interruzione (totale o parziale) o l'alterazione del suo funzionamento. Sono ricompresi anche virus benigni che, pur senza avere effetti distruttivi, possono disturbare il normale funzionamento del sistema, segnalando in vario modo la loro presenza, o programmi worm che riproducendosi incessantemente all'interno della memoria dell'elaboratore in cui vengono inseriti, ne causano il progressivo esaurimento con il conseguente rallentamento delle normali funzioni del sistema;

- utilizzare tecniche di spamming per causare un denial of service di terzi;
- installare software ("trojan horse" o "spyware") nel sistema di terzi al fine di intercettare informazioni riservate o impedire o interrompere le comunicazioni di soggetti pubblici o privati;
- svolgere attività di modifica e/o cancellazione di dati, informazioni o programmi o sistemi informatici di soggetti pubblici o privati;
- svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici o sistemi informatici altrui o di pubblica utilità;
- produrre, importare, vendere, distribuire, mettere a disposizione o in qualsiasi modo procurare a sé o a altri apparecchiature, dispositivi o programmi informatici costruiti o adattati per commettere reati riguardanti strumenti di pagamento diversi dai contanti (ad esempio software volto a produrre carte di credito digitali false o per realizzare truffe on line);
- 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, per ottenere il trasferimento di denaro, valore monetario o moneta virtuale (ad esempio attraverso operazioni di phishing);
- introdurre e/o conservare presso la Società, a qualsiasi titolo e per qualsiasi ragione, documentazione e/o materiale informatico di natura riservata e di proprietà di terzi, salvo che questi siano stati acquisiti con il loro espresso consenso;
- trasferire all'esterno files e qualsiasi documentazione riservata di proprietà della Società.

Tutti i soggetti devono rispettare quanto previsto nella documentazione Privacy adottata dalla Società (informative, istruzioni operative, procedute interne).

Il Titolare del trattamento (ossia la Società nella persona del suo legale rappresentante) deve fornire un'adeguata informazione e formazione sull'utilizzo dei sistemi informatici e sulla normativa privacy.

2. Autenticazione informatica con autorizzazione per livelli

Possono trattare i dati aziendali e utilizzare i sistemi informatici solamente i soggetti formalmente individuati quali persone autorizzate al trattamento o i responsabili esterni del trattamento nominati ai sensi del GDPR e del Codice privacy.

Il Presidente del CdA, con il supporto del Direttore e/o di consulenti esterni, deve garantire:

- un sistema di autenticazione informatica che permetta di accertare l'identità delle persone che accedono al sistema informatico aziendale, evitando così l'accesso ai dati da parte di persone non autorizzate. Per realizzare le credenziali di autenticazione deve essere associato un codice per l'identificazione dell'incaricato all'accesso (username), attribuito dal soggetto che amministra il sistema (e non riattribuibile ad altre persone neppure in tempi diversi), ad una parola chiave riservata (password), conosciuta solamente dall'incaricato, che provvederà ad elaborarla, mantenerla riservata e modificarla periodicamente;
- l'esistenza di procedure per definire le modalità idonee di elaborazione, conservazione, periodico aggiornamento delle "password" di autenticazione e per assicurare la segretezza delle stesse. Devono inoltre essere date istruzioni alle persone autorizzate per la diligente custodia dei dispositivi affidati agli stessi;

- attraverso il sistema di accreditamento degli accessi, un sistema di autorizzazione al fine di circoscrivere le funzioni del sistema informatico alle quali ciascun soggetto autorizzato e, in generale, ciascun utente abilitato, possa accedere in relazione a quanto necessario per lo svolgimento delle proprie mansioni lavorative;
- l'esistenza di procedure per eseguire la verifica periodica e la variazione delle caratteristiche del livello di autorizzazione da parte delle persone autorizzate all'accesso (dovrà prevedersi la variazione del livello in caso di perdita o acquisto di nuovi diritti di accesso ai dati, con conseguente cancellazione o attribuzione di credenziali per operare sui dati). Deve inoltre essere prevista la rimozione dei diritti di accesso al sistema informatico della Società in caso di cessazione del rapporto di lavoro.

3. Sistemi e misure di protezione dei dati e sistemi informatici

Il Presidente del CdA, con il supporto del Direttore e/o di consulenti esterni, deve:

- realizzare e gestire un sistema di protezione di strumenti e dati da malfunzionamenti, attacchi informatici e programmi che contengono virus, con l'adozione di misure idonee e comunque con necessaria adozione e costante aggiornamento di programmi "antivirus" e "firewall";
- adottare ed installare appositi programmi per prevenire la vulnerabilità degli strumenti elettronici e che permettano la verifica di eventuali carenze e inesattezze nella configurazione dei sistemi operativi e dei servizi di rete e di correggere di conseguenza i difetti insiti negli strumenti stessi.

Ogni soggetto della Società deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico mediante virus o mediante ogni altro software aggressivo. Tutti i soggetti aziendali devono quindi:

- mantenere installati e attivi i software impostati per la protezione da virus o altri attacchi informatici;
- controllare il funzionamento dell'antivirus segnalando immediatamente al Direttore eventuali anomalie;
- sospendere ogni elaborazione in corso senza spegnere il computer nonché segnalare prontamente l'accaduto al Direttore, nel caso in cui il software antivirus rilevi la presenza di un virus.

4. Installazione di software

Soltanto i soggetti autorizzati devono essere in possesso delle credenziali di autenticazione che consentano l'installazione di software all'interno dei sistemi informatici della Società.

I soggetti autorizzati che provvedano all'installazione di un qualsiasi software sui sistemi informatici della Società, devono verificare che la stessa sia in possesso della licenza di installazione ed utilizzo del software rilasciata dalla ditta produttrice o di idonea documentazione comprovante la facoltà di libero utilizzo del software stesso, verificando altresì che il software non sia già stato installato su tante postazioni quante consentite dalla licenza stessa.

È fatto divieto a tutti i dipendenti di:

- scaricare da Internet, anche su propri dispositivi privati, programmi senza la preventiva autorizzazione del Direttore;
- effettuare il download di programmi non provenienti da una fonte certa e autorizzata;
- accedere illegalmente e duplicare, riprodurre, utilizzare banche dati senza autorizzazione;
- utilizzare software violando diritti d'autore;
- duplicare ovvero rimuovere i dispositivi di protezione dei programmi;
- detenere a scopo commerciale o imprenditoriale programmi contenuti in supporti non contrassegnati dalla Società Italiana degli Autori ed Editori (SIAE).

5. Invio di comunicazioni informatiche alla Pubblica Amministrazione e per l'accesso a siti della stessa

Il Presidente del CdA deve individuare formalmente i soggetti autorizzati all'utilizzo della "posta elettronica certificata" della Società.

I soggetti che accedono ai siti della Pubblica Amministrazione per l'inserimento di dati ed informazioni della Società od effettuano la comunicazione di tali dati o informazioni a mezzo posta elettronica, devono fornire informazioni e dati veritieri, ricavati da documentazione elaborata da CFLI e prodotta dai soggetti competenti della struttura. Il soggetto che fornisce i dati e informazioni al soggetto autorizzato per la comunicazione alla Pubblica Amministrazione deve siglare i documenti o comunque garantire la corrispondenza ai documenti societari.

Deve essere previsto l'utilizzo esclusivamente dei sistemi informatici della Società per l'accesso alla posta elettronica certificata e ai siti protetti della Pubblica Amministrazione.

Si veda anche il "Protocollo per i rapporti con pubblici ufficiali o incaricati di un pubblico servizio ed organi di controllo" del Modello 231.

6. Utilizzo firma digitale/elettronica

Il Presidente deve individuare formalmente i soggetti autorizzati all'utilizzo della firma digitale/elettronica della Società.

La delega/autorizzazione deve contenere una chiara e precisa indicazione degli atti che potranno essere sottoscritti e dei poteri delegati.

Devono essere previsti meccanismi idonei ad evitare l'utilizzo indebito della smart card da parte di soggetti non autorizzati (es. luogo di custodia della stessa).

7. Protezione delle informazioni riservate della Società e per quelle messe a disposizione del pubblico

Il Presidente del CdA, con il supporto del Direttore, si impegna a porre in essere i seguenti adempimenti:

- prevedere misure di protezione per le informazioni riservate della Società, sia nella fase di trasmissione sia nella fase di memorizzazione e conservazione, in modo che le stesse siano accessibili solo a soggetti determinati e che non possano essere modificate da persone non autorizzate;
- predisporre misure di protezione dell'integrità delle informazioni messe a disposizione su un sistema accessibile al pubblico prevedendo che le stesse possano essere modificate solo da persone autorizzate.

Si veda anche il "Protocollo per la comunicazione di dati ed informazioni societarie" del Modello 231.

8. Utilizzo di immagini, video e musiche, marchi segni di terzi

La Società non deve utilizzare o trasmettere con qualsiasi mezzo fonogrammi o videogrammi di opere musicali, cinematografiche, audiovisive o sequenze di immagini per il quale sia obbligatorio il contrassegno SIAE, prive di tale contrassegno o con contrassegno contraffatto o alterato.

Prima di qualsiasi utilizzo di opere fotografiche, opere cinematografiche e musicali, immagini e contenuti audiovisivi, banche dati, marchi/loghi e segni distintivi di prodotti industriali, il soggetto che intende utilizzare gli stessi deve verificare l'eventuale altrui titolarità di diritti d'autore, diritti di edizione, diritti di sfruttamento, diritti di utilizzazione economica e /o altri diritti di proprietà intellettuale o industriale. Le verifiche devono essere eseguite attraverso l'utilizzo delle apposite banche dati e/o deferendo a professionisti tecnico-legali lo svolgimento delle relative indagini.

Se le verifiche individuano la sussistenza di diritti altrui inerenti a opere/marchi oggetto di indagine, devono essere stipulati specifici accordi per iscritto con il soggetto proprietario o titolare dei relativi diritti di sfruttamento e utilizzazione economica al fine di ottenere lo specifico consenso scritto di utilizzo o apposita manleva da responsabilità. In assenza di tale documentazione ci si deve astenere da qualunque forma di utilizzo e/o riferimento agli stessi.

Ove siano identificati rischi di contraffazione od alterazione, è necessario rinunciare all'utilizzo degli stessi.
Tutta la documentazione (contratto, accordo, consenso scritto, fattura e/o altro titolo) legittimante l'uso di un'opera/ marchio di terzi o la libera utilizzabilità degli stessi deve essere ordinatamente archiviata.
Il soggetto che intende utilizzare l'opera/marchio di terzi deve tenere uno scadenzario della durata del titolo legittimante l'uso degli stessi o dei diritti di licenza e deve verificare che il loro impiego sia conforme e rispetti l'autorizzazione/consenso ricevuti.
Immagini, segni, marchi, e altre opere iconografiche devono essere salvati su cartelle informatiche differenziate in funzione del titolo legittimante l'uso e dei limiti eventualmente previsti nel titolo stesso (contenuti di proprietà della Società, uso libero, differenti vincoli per numero di pubblicazioni, unico utilizzo).
Qualora, in ragione del titolo, sia legittimo un solo utilizzo del contenuto, lo stesso deve essere rimosso una volta utilizzato.

9. Modalità di controllo

Il Presidente del CdA, con il supporto del Direttore e/o di consulenti esterni, nel rispetto di quanto previsto dallo Statuto dei Lavoratori L. 300/70 e dalle altre norme vigenti in materia di tutela dei lavoratori, deve provvedere con periodicità, anche con controlli a campione, a:

- monitorare l'efficacia ed il corretto utilizzo delle misure di sicurezza adottate per gli strumenti elettronici;
- attraverso l'adozione di strumenti automatici di reportistica e di sintesi, individuare i tentativi, riusciti o meno, di accesso non autorizzato al sistema e l'esecuzione di operazioni non corrette, o sospette;
- verificare la sicurezza delle trasmissioni in rete;
- verificare il livello di formazione dei soggetti autorizzati al trattamento.

Il Presidente del CdA, con il supporto del Direttore e/o di consulenti esterni, deve effettuare periodicamente un censimento degli strumenti informatici aziendali e verificare che negli stessi siano presenti solo software autorizzati dalla Società e che sia stato assolto il pagamento dei relativi diritti di licenza. Laddove la gestione delle licenze dei software utilizzati nella Società sia affidata a fornitori esterni, il rinnovo delle stesse dovrà essere formalmente disciplinato nel relativo contratto.
Ove la gestione dei sistemi informatici aziendali sia affidata a fornitori esterni, gli stessi devono immediatamente informare il Presidente del CdA di eventuali incidenti o eventi afferenti la sicurezza informatica della Società, nonché su ogni eventuale anomalia verificatasi nell'utilizzo dei sistemi informatici o dei servizi internet e posta elettronica.
Il Consiglio di Amministrazione deve verificare l'operato dei soggetti intervenuti nel processo e nel caso in cui emergano difformità rispetto al presente protocollo, deve prevedere eventuali azioni correttive e curare che le stesse siano portate a conoscenza del soggetto interessato e che siano attuate.

10. Tracciabilità documentale e conservazione

Per ogni passaggio, richiesta di informazioni, predisposizione di documenti e di relazioni informative, il soggetto che ha svolto tali attività deve siglare i documenti o garantirne la successiva rintracciabilità al fine di agevolare eventuali verifiche e controlli.
Tutti i documenti legati al processo devono essere conservati in ordine presso gli uffici della Società a cura dei soggetti intervenuti a disposizione per le verifiche ed i controlli del caso.

11. Flussi informativi all'OdV

Il Direttore deve informare l'O.d.V. su eventuali incidenti o eventi afferenti la sicurezza informatica della Società, nonché su ogni eventuale anomalia verificatasi nell'utilizzo dei sistemi informatici.

Il Direttore deve informare annualmente l'O.d.V. dell'utilizzo di opere, marchi/loghi e segni distintivi altrui e degli accordi stipulati con il soggetto proprietario o titolare dei relativi diritti di sfruttamento e utilizzazione economica.
Tutti i soggetti coinvolti nel processo sono tenuti a comunicare all'O.d.V. qualsiasi eccezione comportamentale o qualsiasi evento inusuale o suscettibile di incidere sull'effettività od operatività del presente Protocollo. Le azioni correttive intraprese e adottate devono essere comunicate all'O.d.V.
Tutti i soggetti coinvolti devono mettersi a disposizione dell'O.d.V., fornire le eventuali informazioni richieste per iscritto o durante i sopraluoghi non ostacolando le attività di vigilanza svolte dall'O.d.V.

12. Sistema Disciplinare

Eventuali violazioni o inosservanze al protocollo sopra indicato dovranno essere trattate secondo quanto previsto dal "Sistema disciplinare" predisposto in seno alla Parte Generale del presente Modello di organizzazione e gestione.