



INFORMATIVA

Norme generali sull'uso delle postazioni di lavoro e per la gestione delle password.

Riferimenti:

- Regolamento Europeo Generale sulla protezione dei dati personali n. 679/2016 (c.d. "GDPR") e D. Lgs. 196/2003 "Codice in materia di protezione dei dati personali" e s.m.i..

Contenuto:

(1) Postazioni di lavoro

L'utilizzo abituale o saltuario delle postazioni di lavoro (pc, terminali, server, ecc) dovrà avvenire nel pieno rispetto di tutte le norme di legge e delle misure previste per la tutela della privacy e la sicurezza del sistema informatico aziendale. In particolare dovranno essere osservate con scrupolo le seguenti misure specifiche:

- a. L'utilizzo delle postazioni di lavoro è riservato unicamente ai fini aziendali. Nessun uso privato è consentito, salvo che non venga esplicitamente autorizzato per iscritto dai responsabili aziendali. L'uso delle postazioni di lavoro per scopi privati avverrà in ogni caso nel rispetto delle stesse modalità e delle stesse procedure stabilite per l'uso aziendale. In particolare, nessuna deroga è ammessa per il rispetto delle norme di legge e per le misure finalizzate alla tutela della riservatezza, alla continuità ed alla sicurezza del sistema informatico aziendale.
- b. L'accesso alle postazioni di lavoro dovrà essere svolto nel rispetto dei sistemi di autenticazione posti a protezione del sistema informatico. Ciascun utente è responsabile per la tutela delle proprie password di accesso e si impegna a non diffonderne la conoscenza ad alcun soggetto. Per ogni altra direttiva qui non specificata in merito alle password si dovrà fare riferimento alle norme generali per la loro gestione (vedere il Registro aziendale delle attività di trattamento, redatto ai sensi dell'art. 30 del REG. UE n. 679/16).
- c. La postazione di lavoro è conservata dagli utenti nelle medesime condizioni in cui essa è consegnata ad inizio del turno di lavoro o all'atto della presa in carico. Ogni utente è responsabile della manutenzione ordinaria (es. pulizia video, tastiera o mouse, accensione e spegnimento corretti, scansione antivirus periodica, ecc) della postazione a lui assegnata o di cui usufruisce temporaneamente. Particolare cura dovrà essere adottata nella gestione di apparecchiature portatili quali notebook, palmari o simili. Nessuna manomissione è possibile sulla postazione, ivi compresa

l'installazione di apparecchiature o altro hardware non autorizzato. Per qualsiasi necessità occorrerà fare riferimento al responsabile del sistema informatico.

- d. Sulle postazioni di lavoro dovranno essere installati programmi (antivirus, firewall, ecc) posti a protezione delle postazioni stesse e, più in generale, del sistema informatico. Essi non dovranno mai essere disinstallati e dovranno essere soggetti ad aggiornamento costante. Per le postazioni che non dispongano di accessi alla rete Internet e per le postazioni stand-alone dovranno essere messe in atto opportune soluzioni per consentire anche a queste di ricevere gli aggiornamenti necessari (uso di cartelle in rete, aggiornamento manuale, uso di supporti).
- e. In caso di abbandono temporaneo della postazione di lavoro si dovranno abilitare quei sistemi necessari ad impedirne l'uso da parte di terzi non autorizzati (es. salvaschermo con password). In mancanza di tali sistemi si dovrà terminare ogni sessione di lavoro prima di abbandonare la postazione e, nei casi estremi, procedere al suo spegnimento. La postazione va resa inaccessibile o spenta anche al termine dell'orario di lavoro o in caso di assenza prolungata.
- f. Il reinserimento in rete di portatili, specie se provenienti da attività svolte presso clienti, dovrà avvenire solo a condizione che venga effettuata una preventiva scansione antivirus.
- g. Nessun programma o pacchetto d'installazione va inserito, scaricato o installato sulle postazioni di lavoro se non autorizzato. L'installazione di programmi è riservata al responsabile del sistema informatico. Ad esso ci si dovrà rivolgere per la manutenzione dei programmi di ciascuna postazione.
- h. L'uso di supporti di memorizzazione removibili, in lettura o in scrittura, è limitato agli scopi aziendali. In particolare, il salvataggio di dati al di fuori delle procedure di back-up aziendali deve essere autorizzato. La conservazione di tali supporti, laddove possibile, dovrà avvenire negli stessi spazi dedicati al back-up aziendale o, in alternativa, in apposito luogo indicato dal responsabile della privacy e della sicurezza sui dati. Nessun altro utilizzo è possibile per tali supporti e dei dati ivi contenuti al di fuori del ripristino dei dati stessi in caso di bisogno;
- i. in caso di smarrimento o furto di dispositivi informatici, informare tempestivamente il responsabile del sistema informatico ed il Titolare del trattamento dei dati personali avendo cura di comunicare loro quali dati erano contenuti all'interno

L'utente è responsabile delle attrezzature che gli sono affidate in uso e pertanto deve provvedere a mantenerle in completa efficienza segnalando tempestivamente al responsabile del sistema informatico ogni eventuale problema tecnico e, in caso di dubbio, sulla sicurezza della postazione di lavoro.

Ai soli fini di prestare assistenza tecnica informatica ai lavoratori, la Società utilizza alcuni software che permettono all'amministratore di sistema di vedere in tempo reale le attività svolte dal lavoratore all'interno della propria sessione di lavoro ed eventualmente intervenire attivamente. L'attivazione di tale funzionalità può esser richiesta solamente da parte dell'amministratore di sistema e solo quando strettamente necessario per poter svolgere l'attività di assistenza tecnica informatica e deve esser sottoposta ad un preventivo e contestuale consenso del lavoratore.

(2) Gestione delle password

Ovunque sia indispensabile l'utilizzo di password per l'autenticazione di accessi al sistema informatico o la protezione di file riservati, la gestione delle stesse dovrà avvenire nel rispetto di tutte le norme di legge e delle misure previste per la tutela della privacy e la sicurezza del sistema informativo aziendale. In particolare dovranno essere osservate con scrupolo le seguenti misure specifiche:

- a) Tutte le password aziendali sono considerate informazioni altamente confidenziali che non possono essere comunicate ad alcun soggetto non autorizzato. Le password personali sono segrete e non devono essere comunicate ad alcun soggetto. Le password personali che vincolano l'utilizzo di una risorsa aziendale (es. password di bios, password uniche di amministrazione) oppure di un file od un archivio elettronico devono essere consegnate in busta chiusa al responsabile aziendale delle password affinché possa utilizzarle in caso di bisogno.
- b) Ogni singolo soggetto è responsabile della tutela alla segretezza delle password aziendali di cui ha conoscenze; la tutela della segretezza delle password personali è in carico esclusivamente al singolo utente. Le password personali non vanno scritte o annotate.
- c) Le password devono essere lunghe almeno otto caratteri e non debbono contenere elementi facilmente riconducibili al singolo utente cui si riferiscono (es. nome, cognome, data nascita, ecc) né devono essere tratte da elementi troppo evidenti rispetto al contesto ambientale o aziendale. Ove non fosse possibile l'utilizzo di otto caratteri si dovrà utilizzare il numero massimo fra quelli disponibili. Le password devono avere un sufficiente livello di complessità, devono cioè comprendere lettere, numeri e caratteri speciali in maiuscolo e minuscolo alternati fra loro.
- d) Le password devono essere cambiate con una frequenza almeno semestrale. In caso di trattamenti di dati qualificabili come "particolari categorie di dati" (ex art. 9 del Reg. UE n. 679/16) o giudiziari (ex art. 10 del Reg. UE n. 679/16) le password vanno cambiate con frequenza almeno trimestrale.
- e) Le password già utilizzate non vanno più usate in successivi cambiamenti delle parole di accesso. Ad ogni rotazione le nuove password devono essere originali. Laddove è possibile le nuove password non devono essere frutto di elaborazioni basate sulle vecchie, né derivare da regole predefinite di composizione.

Bra, 6/08/2018


casa di cura
città di bra
IL PRESIDENTE
Dr. GIACOMO BRIZIO