

DISCIPLINARE AZIENDALE IN MATERIA DI UTILIZZO DEGLI STRUMENTI INFORMATICI IN OSSERVANZA DEL PROVVEDIMENTO GENERALE DEL GARANTE DEL 01.03.2007

RE:Lab s.r.l., nella qualità di Titolare, ai sensi dell'articolo 4, comma 1, lettera f) del Codice in Materia di Protezione dei Dati Personali (di seguito Codice), La informa che i Suoi dati personali (da Lei forniti per obbligo contrattuale, ovvero altrimenti acquisiti nel rispetto delle disposizioni legislative e contrattuali vigenti) inerenti, connessi e/o strumentali al suo rapporto di lavoro (subordinato e/o di collaborazione), potranno formare oggetto di trattamento per finalità connesse alle reciproche obbligazioni derivanti dal rapporto di lavoro con Lei intercorrente, nel rispetto della normativa sopra richiamata e degli obblighi di riservatezza.

Per trattamento di dati personali si intende la loro raccolta, registrazione, organizzazione, conservazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, comunicazione, diffusione, cancellazione e distruzione, ovvero la combinazione di due o più di tali operazioni, anche attraverso strumenti automatizzati atti a memorizzare, gestire e trasmettere i dati stessi, utilizzando strumenti idonei a garantire la sicurezza e la riservatezza. Tra questi strumenti, alcuni Le vengono dati in uso per espletare la Sua attività lavorativa (ad esempio connessione di rete e servizio di posta elettronica).

L'utilizzo delle risorse informatiche, telematiche e del patrimonio informativo della nostra Società deve pertanto ispirarsi sempre al principio della diligenza e correttezza, comportamenti che il dipendente, collaboratore e/o stagista è sempre tenuto ad adottare nell'ambito del rapporto di lavoro: ne consegue che ogni utilizzo delle apparecchiature, degli elaboratori, delle reti e dei dati non avente finalità strettamente professionali deve essere limitato e di natura occasionale.

Poiché alcuni comportamenti possono mettere a rischio la Sicurezza e l'immagine aziendale anche nello svolgimento della normale attività lavorativa, di seguito vengono richiamate semplici regole procedurali finalizzate non tanto a censurare comportamenti consapevolmente scorretti e già di per sé proibiti, quanto ad evitare condotte inconsapevolmente rischiose.

A seguito dell'emanazione, da parte del Garante per la Protezione dei Dati Personali, del provvedimento generale del 1 marzo 2007 avente ad oggetto "Linee guida del Garante per posta elettronica e Internet" ed al fine di conciliare l'esigenza di tutela della Sua privacy ed il corrispondente potere/dovere del Titolare di assicurare la funzionalità e il corretto impiego degli strumenti informatici da parte Sua, RE:Lab s.r.l. ha adottato il presente Disciplinare interno che

regolamenta, pur nel rispetto dei principi di pertinenza e non eccedenza, le modalità di utilizzo da parte Sua dei servizi informatici aziendali, nonché le attività di controllo che può legittimamente effettuare il Titolare sui ed attraverso i medesimi strumenti tecnologici.

1. Posta Elettronica

Il servizio di posta elettronica aziendale è disponibile per ogni dipendente, collaboratore e/o stagista in forma centralizzata e protetta. L'accesso a tale servizio è possibile sia mediante un *email client*, sia attraverso la *webmail*, e può essere effettuato anche dall'esterno della Intranet attraverso protocolli di comunicazione sicuri (crittografia).

E' fatto divieto di utilizzare le caselle di posta elettronica aziendale per l'invio di messaggi personali, salvo diversa ed espressa autorizzazione da parte della Direzione.

L'utilizzo di questo servizio deve ottemperare alle regole di *Netiquette* ad esso applicabili.

La composizione dell'indirizzo di posta elettronica aziendale per ciascun dipendente, collaboratore e/o stagista, fatta eccezione per eventuali casi di omonimia, avviene con l'iniziale del nome e il cognome, col punto ortografico come carattere di separazione e *re-lab.it* come dominio; nel caso di John Doe, per esempio, risulterebbe j.doe@re-lab.it.

E' stata predisposta la mailing list staff@re-lab.it per l'invio di comunicazioni ufficiali tra il personale dell'azienda, utilizzabile da tutti e soli gli indirizzi di posta elettronica aziendali; i messaggi inviati a questa mailing sono soggetti ad un meccanismo di moderazione per cui, una volta spediti, rimangono sul server di posta in attesa dell'approvazione di uno dei membri del CDA e possono essere rimbalzati al mittente se non ritenuti idonei.

2. Utilizzo dei dispositivi informatici e della Intranet

L'accesso a qualunque servizio aziendale è sempre protetto da una o più password, così come previsto dalle misure minime di sicurezza disciplinate dal Codice della Privacy ed in particolare dall'Allegato B, denominato "Disciplinare tecnico in materia di misure minime di sicurezza".

E' reso disponibile a ciascun dipendente, collaboratore e/o stagista un particolare account, detto "certalizzato", mediante il quale è possibile accedere ai principali servizi informatici aziendali (posta e agende elettroniche, aree condivise per lo scambio di file, repository di codice ed altro ancora); data la sua criticità, questo account deve avere una password che rispetti i requisiti requisiti minimi di robustezza espressi [qui](#) e che sia periodicamente sostituita.

Tutte le password sono personali: non devono assolutamente essere divulgate a terzi e devono essere custodite dall'assegnatario con la massima diligenza.

Il dipendente, collaboratore e/o stagista ha altresì l'obbligo di comunicare la password adottata ad ogni sua variazione in busta chiusa firmata e datata di suo pugno, al Responsabile dei sistemi informativi. Questi, in caso di emergenza e/o di assenza del lavoratore, avrà il diritto di accedere ad ogni dispositivo o servizio cui egli abbia accesso, per esigenze di carattere lavorativo, utilizzando le password comunicate.

I permessi per l'accesso ai servizi informatici aziendali saranno conferiti al personale in base alle reali necessità di fruizione.

E' tassativamente proibito installare programmi senza previa autorizzazione da parte del Responsabile dei sistemi informativi.

Le aree di condivisione dei dati e, in generale, tutti i dispositivi di memorizzazione devono essere utilizzati esclusivamente per scopi di natura aziendale. Su queste unità vengono svolte regolari attività di controllo, amministrazione e backup da parte del Responsabile dei sistemi informativi; questi, in qualunque momento, può procedere alla rimozione di tutti i dati ritenuti pericolosi per la sicurezza o non inerenti all'attività lavorativa.

E' essenziale una corretta gestione delle aree di condivisione, in particolare provvedendo alla cancellazione dei file obsoleti o inutili ed evitando la replicazione dei dati. L'archiviazione delle informazioni deve essere effettuata secondo quanto previsto delle procedure presenti nel manuale di qualità.

E' necessario impedire l'accesso di terzi a qualunque dispositivo in dotazione, avvalendosi degli eventuali sistemi di protezione presenti (es. blocco dello schermo dei PC con codice di accesso).

L'operatore avrà cura di effettuare la stampa dei dati solo se necessario e di ritirarla immediatamente dai vassoi delle stampanti comuni. Si eviterà in ogni modo e per quanto possibile di dislocare stampanti e fax in aree accessibili a soggetti non abilitati al trattamento dei dati e non presidiate (per esempio: corridoi, sale d'attesa, ecc.).

3. Utilizzo di Internet e dei relativi servizi

L'utilizzo improprio di alcuni servizi Internet, ancorché nell'ambito della normale attività aziendale, può essere fonte di minacce alla sicurezza dei dati e all'immagine aziendale.

Seguono alcuni esempi di semplici regole per il corretto utilizzo della Rete:

- ⌘ è da evitare il trasferimento (upload e/o download) di file e/o programmi, anche gratuiti, se non per esigenze strettamente aziendali e comunque senza la previa esplicita autorizzazione del Responsabile dei sistemi informativi;

- ▲ è vietata la fruizione di servizi online non aziendali quali forum, chat, blog e, più in generale, qualunque servizio attuale o futuro non inerente all'attività lavorativa.

4. Attività di formazione

La Società predispone regolari momenti formativi ed informativi per garantire a tutti gli incaricati il massimo aggiornamento in merito ai rischi, alle procedure operative, alla prevenzione dei danni e, più in generale, alle problematiche relative alla sicurezza in materia di trattamento dei dati.

Lei potrà comunque rivolgersi, per ogni chiarimento in merito, al designato Legale Rappresentante individuato nella persona dell'Ing. Fabio Pagliai.

Copia conforme all'originale del presente Disciplinare è stata affissa nella bacheca aziendale in formato cartaceo ed inserita in formato elettronico all'interno del sito aziendale nella sezione Privacy.

Tutti i dipendenti, collaboratori e/o stagisti prendono visione di tale documento in sede di incontro esplicativo.

Reggio Emilia, lì 01/09/2011