

- 1) **SCOPO**
- 2) **CAMPO APPLICAZIONE**

| | | | | | |
|------|--------------------|----------|-----------|------------|-----------|
| 1 | Modifica Cartiglio | 06/06/11 | IT | DIG | DIG |
| 0 | Emissione | 31/01/10 | IT | DIG | DIG |
| Rev. | Motivazione | Data | Preparato | Verificato | Approvato |

1) SCOPO

Qualunque genere di controllo (generalizzato e/o specifico, diretto o indiretto) sul lavoratore e sull'uso di PC/internet/risorse informatiche di ogni genere, deve essere esplicitato e previsto in apposito regolamento informatico come disciplinato dal Provvedimento del 1 marzo 2007, emanato dall'Autorità Garante in materia di privacy, nonché tenuto conto delle vigenti norme sulla tutela del lavoratore (vedasi a titolo esemplificativo e non esaustivo l'art. 4 L. 300/70)

“REGOLAMENTO INFORMATICO INTERNO VALIDO AI SENSI DEL D.LG. 196/03 PER FINI FORMATIVI IN MATERIA DI PROTEZIONE DEI DATI PERSONALI”

2) CAMPO DI APPLICAZIONE

Utilizzo strumentazione

1. Non è consentito installare sulla strumentazione in uso, hardware fisso o removibile qualora ciò non risulti espressamente richiesto ed autorizzato dalla Società.
2. In caso di allontanamento dalla propria postazione hardware, attivare il salva-schermo protetto da password.
3. Sui PC dotati di scheda audio e/o di lettore CD non è consentito l'ascolto di programmi, files audio o musicali, se non a fini prettamente lavorativi.
4. Qualora si rendessero necessarie modifiche alle configurazioni impostate sul PC in uso, occorre darne comunicazione al Sig. Enrico Samorè.

Accesso ed uso dei sistemi

1. Il dipendente si connette alla rete tramite autenticazione univoca personale.
2. Le credenziali di autenticazione alla rete devono essere custodite e preservate dalla conoscibilità di colleghi o soggetti esterni alla Società.
3. In nessun caso devono essere annotate password in chiaro sia su supporto cartaceo che informatico.
4. I requisiti minimi di complessità delle password sulla base della vigente normativa privacy sono:
 - redazione con caratteri maiuscoli e/o minuscoli;
 - composizione con inclusione di simboli, numeri, punteggiatura e lettere;
 - caratteri non inferiori ad 8 (ad eccezione dei sistemi operativi che non supportano tali requisiti);
 - password non agevolmente riconducibile all'identità del soggetto che la gestisce. Pertanto, la password non deve essere basata su informazioni personali, riferimenti familiari o comunque dati inerenti direttamente il soggetto titolare della password stessa.
5. Qualora l'intestatario della password ritenga che un soggetto non autorizzato possa essere venuta a conoscenza della propria password, dovrà provvedere immediatamente a cambiarla dandone comunque comunicazione al custode delle password (sig.ra Ballani Micaela).
6. Non debbono essere utilizzate nella configurazione delle caselle di posta elettronica le opzioni di "compilazione automatica" o remember password, presenti nei browser o in altre applicazioni.
7. Il dipendente ha l'obbligo di non alterare la funzione "cambio password" che obbliga a modificare la password con cadenza semestrale.

Installazione programmi

1. Sul pc in uso non devono essere installati programmi non attinenti all'attività lavorativa e che non siano ufficialmente autorizzati dall'azienda.

Utilizzo supporti magnetici e dati

1. È fatto obbligo conservare, custodire e controllare i supporti informatici removibili contenenti dati, informazioni, notizie o immagini di attinenza aziendale, affinché nessun soggetto terzo ne prenda visione o possesso.
2. Qualsiasi file estraneo all'attività lavorativa o non espressamente autorizzato, non può, essere salvato sul PC in uso del dipendente.
3. Tutti i files di provenienza incerta o esterna, ancorché attinenti all'attività lavorativa, devono essere sottoposti al controllo e relativa autorizzazione all'utilizzo da parte del sig. Enrico Samorè.

Utilizzo rete interna

1. La rete interna, istituita appositamente per permettere collegamenti funzionali tra utenti che prestano servizio all'interno della struttura lavorativa, non può esser utilizzata per scopi diversi da quelli ai quali è destinata.
2. Qualora nella rete interna debbano circolare dati, notizie ed informazioni aziendali, deve essere premura di ciascun dipendente preservare gli stessi dalla conoscibilità di terzi soggetti non espressamente autorizzati ad aver notizia di tali dati.

Utilizzo rete esterna Internet

- 1) E' fatto divieto memorizzare dalla rete documenti, file o dati comunque non attinenti lo svolgimento delle attività aziendali, in particolare:
 - non è consentito navigare in siti non attinenti allo svolgimento delle mansioni assegnate;
 - non è consentita l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo nei casi direttamente autorizzati dall'azienda e con il rispetto delle normali procedure di acquisto;
 - è vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;
 - non è permessa la partecipazione, per motivi non professionali, a Forum, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest book anche utilizzando pseudonimi (o nicknames) potendo esporre a rischi di sicurezza la rete aziendale;
- 2) Si rende noto che la Società non ha attivato alcun sistema di monitoraggio della navigazione aziendale. Qualora fosse necessario attivare tali sistemi, l'azienda si impegna a darne immediata comunicazione secondo le previsioni di cui al Provvedimento del Garante in materia di trattamento dati personali, Provvedimento del 1 marzo 2007, circa le modalità con cui si effettua monitoraggio generalizzato ed anonimo dei log di connessione; così come le modalità di archiviazione e tempi di conservazione dei log risultanti.
- 3) Eventuali attivazioni di controlli specifici, monitoraggi o registrazioni di log contenenti traccia di ogni operazione di collegamento effettuata dall'interno della rete societaria verso Internet, saranno preventivamente notificate.

Accesso alla rete aziendale da remoto

- 1) Il software client che permette l'accesso da remoto deve essere preventivamente autorizzato ed installato dall'Amministratore di Sistema.
- 2) L'utilizzo da remoto nella rete aziendale è sottoposto allo stesso regolamento interno informatico.

Utilizzo del fax

- 3) Si raccomanda di non lasciare documenti incustoditi presso le postazioni di fax all'atto dell'invio.
- 4) Qualora il dipendente sia prossimo a ricevere atti contenenti dati o informazioni riservate via fax, avrà cura di monitorare la postazione fax e preservare - limitatamente alle oggettive possibilità - la conoscibilità di tali dati o informazioni, da parte di terzi non autorizzati.

Utilizzo posta elettronica

1. Le caselle di posta elettronica date in uso al dipendente sono destinate ad un utilizzo di tipo aziendale.
2. Si rappresenta che:
 - non è consentito inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica, o che costituiscano comunque condotta illecita;
 - non è consentito l'utilizzo dell'indirizzo di posta elettronica aziendale per la partecipazione a dibattiti, Forum, newsletter o mail-list, non attinenti l'attività lavorativa.
3. In caso di assenza, al dipendente sono posti a disposizione apposite funzioni di sistema che consentano di inviare automaticamente messaggi di risposta.
4. E' fatto divieto di divulgare le notizie, i dati e qualsiasi altra informazione appresa in occasione della ricezione o invio di posta elettronica, in quanto coperte dal segreto professionale cui sono tenuti i dipendenti in ottemperanza agli obblighi di fedeltà e correttezza.
5. I messaggi di posta elettronica saranno memorizzati tramite back up giornaliero programmato su nastro magnetico. L'accesso al server di posta ed ai back up è possibile unicamente all'amministratore di sistema, nell'eventuale necessità, a personale incaricato.
6. I soggetti autorizzati a seguire le procedure di cui al punto precedente, sono determinati secondo le capacità e requisiti tecnici posseduti.

Gestione, conservazione e controllo dei dati informatici

È fatto divieto applicare sistemi di crittografia, codificazione e simili ai dati se non espressamente richiesto dalla Società secondo la tipologia di dato o documento.

Segreto professionale

Il dipendente/collaboratore non può divulgare, pubblicare o comunicare in alcun modo a terzi, direttamente o indirettamente, in toto o in parte, le informazioni apprese in occasione dello svolgimento delle mansioni per le quali è stato assunto dalla società, né potrà usarle, sfruttarle o disporne in proprio o tramite terzi.

Gli obblighi del dipendente/collaboratore previsti in questo capo non termineranno all'atto di cessazione del rapporto di lavoro, se non in riferimento a quelle specifiche parti delle informazioni che il dipendente possa dimostrare che erano già di pubblico dominio al momento della conclusione del rapporto, o che lo sono diventate in seguito per fatto a lui non imputabile.

Riservatezza dati

Premesso che per «Informazioni Riservate» si intendono tutte le informazioni di qualsivoglia natura riferite o apprese in occasione dello svolgimento di mansioni per le quali il soggetto è stato assunto dalla società, il dipendente si impegna a considerare le Informazioni Riservate come strettamente private e riservate e ad adottare tutte le misure necessarie per non pregiudicare la riservatezza di tali informazioni;

Il dipendente \ collaboratore si impegna ad utilizzare le Informazioni Riservate unicamente allo scopo di effettuare lo svolgimento dell'attività cui è preposto e di conseguenza a non usare tali informazioni in alcun modo che arrechi danno alla società, né per alcun altro scopo di qualsiasi natura;

Gli impegni di cui al presente capo non proibiscono di comunicare Informazioni Riservate:

- ad amministratori e dipendenti, anche di società nostre controllate, avvocati, revisori, banche o altri nostri consulenti ai quali la conoscenza di tali Informazioni è necessaria al fine dell'espletamento di attività funzionali alla società;
- a soggetti diversi da quelli specificati alla precedente lettera a), qualora ciò sia stato autorizzato dalla Società;

L'obbligo di riservatezza non opera in caso di Informazioni Riservate:

- che al momento in cui vengono rese note siano di pubblico dominio;
- che diventino di pubblico dominio dopo essere state rese note per causa non imputabile al dipendente;

L'impegno di riservatezza di cui al presente capo si protrarrà anche dopo la cessazione del rapporto di lavoro e sino a quando le informazioni in oggetto non saranno rese di pubblico dominio.

Applicazione ed interpretazione del presente regolamento

Per qualsiasi dubbio relativo all'applicazione pratica o all'interpretazione del presente regolamento, il dipendente può rivolgersi al Titolare del trattamento dei dati aziendali, sig. Arzilli Giovanni.

Disciplina deroghe e modifiche del presente regolamento

Qualora al presente regolamento la Società intenda apporre modifiche, queste saranno applicate dandone conoscenza immediata al dipendente.

Deroghe o modifiche di uno o più punti del presente regolamento, non rendono invalidi gli altri punti.