NICO SOCCORSO ONLUS

REGOLAMENTO SICUREZZA INTERNO VALIDO AI SENSI DEL D.LG. 196/2003 E 679/2016 EU PER FINI FORMATIVI IN MATERIADI PROTEZIONEDEI DATI PERSONALI

I lavoratori dipendenti in ottemperanza dei doveri di diligenza, obbedienza (art. 2104 c.c.) e fedeltà all'azienda (art. 2105 c.c.), nonché i lavoratori volontari sono tenuti all'osservanza ed al rispetto del presente regolamento, nonché alla segnalazione di qualsiasi informazione o circostanza che possa compromettere o violare il rispetto del sistema di gestione della privacy aziendale.

Il Titolare del Trattamento dei dati è **NICO SOCCORSO ONLUS** con sede in Migliarino (Fe) via Del Parco n. 1 in persona del legale rappresentante pro tempore, Presidente dell'Associazione, dato di contatto: segreteria@nicosoccorso.it,

Utilizzo strumentazione

a) Il Personal Computer affidato al dipendente è uno **strumento di lavoro**. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

b) E' fatto divieto di installare sulla strumentazione aziendale in uso hardware fisso o removibile (ad esempio modem) qualora ciò non risulti espressamente richiesto ed autorizzato dal Titolare.

c) Il Titolare si riserva di eliminare qualsiasi elemento hardware la cui installazione non sia stata appositamente prevista o autorizzata.

d) In caso di allontanamento dalla propria postazione hardware, è fatto obbligo al dipendente di attivare il salva-schermo protetto da password.

e) 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.

f) Qualora si rendessero necessarie modifiche alle configurazioni impostate sul PC in uso, occorre darne comunicazione a coloro che si occupano della amministrazione pc (MICHELE GARDIN)

1) Accesso ed uso dei sistemi

a) Il dipendente si connette alla rete tramite autenticazione univoca personale.

b) Le credenziali di autenticazione alla rete devono essere custodite e preservate dalla conoscibilità di colleghi o soggetti esterni alla Società. In nessun caso devono essere annotate password in chiaro sia su supporto cartaceo che informatico.

c) I requisiti minimi di complessità delle password sulla base della vigente normativa privacy sono:

1.i) Redazione con caratteri maiuscoli e/o minuscoli;

1.ii) Composizione con inclusione di simboli, numeri, punteggiatura e lettere;

1.iii) Numero di caratteri non inferiori a 8 (ad eccezione dei sistemi operativi che non supportano tali requisiti);

1.iv) 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.

d) Qualora l'intestatario della password ritenga che un soggetto non autorizzato possa essere venuto a conoscenza della propria password, dovrà provvedere immediatamente a cambiarla, dandone comunque comunicazione al titolare del trattamento.

e) 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.

f) Il dipendente ha l'obbligo di non alterare la funzione "cambio password" che obbliga a modificare la password con cadenza trimestrale.

2) Installazione programmi

a) Sul pc in uso non devono essere installati programmi che non siano ufficialmente forniti da coloro che si occupano della amministrazione pc (MICHELE GARDIN)

b) Si ricorda che costituiscono illecito penale le condotte consistenti nella illecita duplicazione o riproduzione di software ai sensi della legge sul diritto d'autore n. 633/41 come novellata.

3) Utilizzo supporti magnetici e dati

a) 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.

b) Qualsiasi file estraneo all'attività lavorativa o non espressamente autorizzato, non può, nemmeno in via transitoria, essere salvato sul pc in uso del dipendente.

c) Tutti i file di provenienza incerta o esterna, ancorché attinenti all'attività lavorativa, devono essere sottoposti al controllo e relativa autorizzazione all'utilizzo da parte del responsabile.

4) Utilizzo rete interna

a) 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.

b) 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.

5) Utilizzo rete esterna Internet

a) È fatto divieto memorizzare dalla rete documenti, file o dati comunque non attinenti lo svolgimento delle attività aziendali, in particolare:

1.i) Non è consentito navigare in siti non attinenti allo svolgimento delle mansioni assegnate;

1.ii) Non è consentita l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di *remote banking,* acquisti *online* e simili, salvo nei casi direttamente autorizzati dal titolare e con il rispetto delle normali procedure di acquisto;

1.iii) È vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;

1.iv) 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.

b) Si rende noto che la Società ha attivato sistemi di monitoraggio della navigazione aziendale secondo le previsioni di cui al Provvedimento del Garante in materia di trattamento dati personali, Provvedimento del 1 marzo 2007, effettuando monitoraggio generalizzato ed anonimo dei log di connessione.

a.i) Gli archivi di log risultanti da questo monitoraggio contengono traccia di ogni operazione di collegamento effettuata dall'interno della rete societaria verso Internet.

a.ii) Eventuali attivazioni di controlli specifici saranno preventivamente notificate.

a.iii) I log di connessione di cui sopra, saranno conservati per novanta giorni.

6) Utilizzo del fax

a) Si raccomanda di non lasciare documenti incustoditi presso le postazioni di fax all'atto dell'invio.

b) 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.

7) Utilizzo posta elettronica

a) Le caselle di posta elettronica date in uso al dipendente sono destinate ad un utilizzo di tipo aziendale.

b) Si rappresenta che:

1.i) 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;

1.ii) 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.

c) In caso di assenza, al dipendente sono posti a disposizione apposite funzioni di sistema che consentano di inviare automaticamente messaggi di risposta.

d) 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.

e) La posta elettronica diretta all'esterno della rete informatica aziendale può essere intercettata da estranei e, dunque, è preferibile non usarla per inviare documenti di lavoro "Strettamente Riservati".

f) I messaggi di posta elettronica saranno memorizzati seguendo le seguenti procedure e tempistiche: _____

g) Alla fine della giornata lavorativa il lavoratore stampa le mail relative ai clienti/fornitori d'interesse condiviso.

8) Gestione, conservazione e controllo dei dati informatici

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

9) Segreto professionale

a) Il dipendente 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 dal datore di lavoro, né potrà usarle, sfruttarle o disporne in proprio o tramite terzi.

b) Gli obblighi del dipendente 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.

10) Riservatezza dati

a) 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.

b) Il dipendente 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.

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

1.i) a commercialisti, avvocati, revisori, banche o altri consulenti ai quali la conoscenza di tali Informazioni è necessaria al fine dell'espletamento di attività funzionali alla Società;

1.ii) a soggetti diversi da quelli specificati alla precedente lettera a), qualora ciò sia stato autorizzato dal Titolare;

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

1.iii) che al momento in cui vengono rese note siano di pubblico dominio;

1.iv) che diventino di pubblico dominio dopo essere state rese note per causa non imputabile al dipendente.

e) 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.

11) Applicazione ed interpretazione del presente regolamento

a) Per qualsiasi dubbio relativo all'applicazione pratica o all'interpretazione del presente regolamento, il dipendente può rivolgersi al titolare del trattamento.

12) Non osservanza della normativa aziendale

a) Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

13) Aggiornamento e revisione

a) Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Le proposte verranno esaminate dalla Direzione. Il presente Regolamento è soggetto a revisione con frequenza annuale. Delle modifiche applicate verrà data conoscenza immediata al dipendente.

14) Disciplina deroghe e modifiche del presente regolamento

a) Qualora al presente regolamento la Società intenda apporre deroghe o modifiche, queste verranno comunicate prontamente al personale.

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

APPENDICE I: norme generali per la sicurezza degli archivi cartacei

Al fine di accentuare la sicurezza degli archivi cartacei, vengono definite le seguenti ulteriori norme di prassi:

1. A fine giornata o in caso di assenza programmata, il personale dovrà provvedere a liberare le scrivanie da documenti contenenti dati personali, archiviandoli in cassetti o armadi protetti da chiusure a seconda della necessità di consultarli in breve periodo. Tale procedura non è necessaria qualora possa essere chiuso direttamente a chiave l'ufficio.
2. Il personale dovrà provvedere a chiudere a chiave la porta dei singoli uffici, al termine della giornata lavorativa. Le chiavi saranno conservate a cura dei lavoratori, portate nel proprio domicilio e riportate la mattina seguente. Durante le assenze programmate dei lavoratori, la chiave verrà consegnata al collega d'ufficio, se presente o al titolare;
3. Il titolare provvederà a inserire e a disattivare l'allarme in loco o da remoto;
4. Le pulizie degli uffici, verranno eseguite dall'impresa fornitrice, alla presenza del titolare.
5. Alla presenza di clienti, fornitori e altro personale esterno, i dipendenti, dovranno provvedere a riporre le cartelle di lavoro negli armadi chiusi;

APPENDICE II: Altre Norme comportamentali

Alla presenza di clienti, fornitori e altro personale esterno, il dipendente dovrà avere cura di non effettuare conversazioni telefoniche dalle quali possano essere forniti, anche incidentalmente, dati sensibili.

CONSEGNA BUSTE PAGA : Adottare opportune cautele a tutela della riservatezza che possono consistere, ad esempio, nel piegare e spillare il cedolino, nell'imbustarlo o nell'apporvi una copertura delle parti più significative che non riguardino dati di comune conoscenza (generalità, ufficio di appartenenza, ecc.), ovvero nell'introdurre una cd. "distanza di cortesia" agli sportelli".

Luogo, data

Firma per presa visione (tutti i dipendenti e volontari)

_____