REGOLAMENTO INFORMATICO INTERNO

Strada Panni, 199 - 41125 Modena CF 80009750367 - P.IVA 02008920361 tel. 059 399.911 -
fax 059 399.902 e-mail direzione@charitasasp.it www.charitasasp.it

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 nome sulla tutela del lavoratore (vedasi a titolo esemplificativo e non esaustivo l'art. 4 L. 300/70).

Premessa

Le nuove tecnologie informatiche, ed in particolare il libero accesso alla rete internet dai Personal Computer, espone l'ASP Charitas ai rischi di un coinvolgimento sia patrimoniale che penale, con possibili ripercussioni alla sicurezza e all'immagine dell'Azienda stessa.

L'utilizzo delle risorse informatiche e telematiche Aziendali è quindi diventato parte integrante del rapporto di lavoro e perciò dev'essere improntato ai principi della diligenza e correttezza.

Ciò detto, l'ASP Charitas ha altresì adottato il presente regolamento, al fine di evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati, disciplinando le condizioni per il corretto utilizzo degli strumenti informatici da parte dei dipendenti e riportando informazioni utili per comprendere cosa può fare ogni dipendente per contribuire a garantire la sicurezza informatica di tutta l'Azienda.

1. Utilizzo strumentazione

- II Personal Computer affidato al dipendente è uno strumento di lavoro, Ognuno è responsabile dell'utilizzo delle dotazioni informatiche ricevute in Assegnazione. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.
- È fatto divieto installare sulla strumentazione in uso, hardware fisso o removibile (ad esempio chiavette per connessione ad internet) qualora ciò non risulti espressamente richiesto ed autorizzato dalla Direzione.
- La Direzione si riserva di eliminare qualsiasi elemento hardware la cui installazione non sia stata appositamente prevista o autorizzata.
- In caso di allontanamento dalla propria postazione hardware, è fatto obbligo al dipendente di bloccare la postazione, utilizzando l'apposito comando di MS Windows "Blocca"
- Qualora si rendessero necessarie modifiche alle configurazioni impostate sul PC in uso, occorre darne comunicazione alla Direzione o ad un soggetto appositamente delegato.
- Le informazioni archiviate con strumenti informatici devono essere esclusivamente quelle previste dalla legge e, o necessarie all'attività lavorativa.

2. Accesso ed uso dei sistemi

- Il dipendente si connette alla rete tramite autenticazione univoca personale.
- Le credenziali di autenticazione alla rete devono essere custodite e preservate dalla conoscibilità di colleghi o soggetti esterni alla Società (familiari ad esempio).

- In nessun caso, sia su supporto cartaceo che informatico, devono essere annotate password in chiaro.
- 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 numeri, lettere e caratteri speciali;
  - non meno di 8 caratteri;
  - 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.
- Qualora l'intestatario della password ritenga che un soggetto non autorizzato possa essere venuto a conoscenza della propria password, dovrà provvedere immediatamente a cambiarla comunicando l'avvenuto al responsabile dei sistemi informativi.
- In caso di prolungata assenza (almeno una settimana) dell'operatore e per urgenze/necessità operative, è necessario rilasciare alla Direzione o ad un soggetto appositamente incaricato), le credenziali d'accesso al computer di pertinenza. Dette credenziali, potranno essere comunicate a chi dovesse avere la necessità di accedere al computer del dipendente assente, registrandone gli accessi. In tale eventualità, trattandosi comunque di un'ipotesi di utilizzo di uno strumento di lavoro personale, l'utilizzo del computer dell'operatore assente, sarà limitato nel tempo e consentito unicamente per esigenze operative aziendali (es. file, documenti, procedure, programmi ecc. che si trovano solo in quel computer).
- Nel caso in cui l'operatore non abbia la possibilità di comunicare le credenziali, sarà la stessa Direzione o un soggetto appositamente incaricato a crearne di nuove per poter accedere al computer, ripristinando le originali al rientro dell'operatore interessato.

3. Installazione programmi

- Sul pc in uso non devono essere installati programmi che non siano stati previamente autorizzati dalla Direzione o da soggetto appositamente incaricato.
- La Direzione, peraltro, ricorda all'utilizzatore, 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.
- È facoltà dei soggetti appositamente incaricati, procedere alla rimozione di ogni file o applicazione sia sui PC del personale, sia sulle unità di rete, che venga ritenuta pericolosa per la Sicurezza.

4. Utilizzo supporti magnetici e dati

- 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.
- Qualsiasi file estraneo all'attività lavorativa o non espressamente autorizzato, non può, nemmeno in via transitoria, essere salvato sul pc in uso del dipendente.
- 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 della Direzione o di un soggetto appositamente incaricato.

5. Utilizzo rete interna

- 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.
- 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.
- L'accesso alla rete aziendale è protetto da password; per l'accesso deve essere utilizzato il proprio profilo personale (username e password).
- È vietato condividere cartelle in rete sia dotate di password, sia sprovviste di password se non dietro esplicita e formale autorizzazione del responsabile dei sistemi informativi.
- È vietata l'installazione non autorizzata di modem che sfruttino il sistema di comunicazione telefonico per l'accesso a banche dati esterne o interne all'azienda.
- È vietato connettere alla rete interna dispositivi informatici (Notebook, smartphone, tablet, ecc.) non di proprietà della ASP Charitas se non dietro esplicita e formale autorizzazione della Direzione o del Resp. dei Sistemi Informativi.
- E' vietato monitorare ciò che transita in rete [log d'accesso[1] e chiusura (log in e log out), attività informatiche, registro eventi, visualizzazioni ecc.] se non con le specifiche precise e particolari autorizzazioni da far pervenire al Resp. dei Sistemi Informativi, da parte delle Autorità autorizzate ai controlli (Es. Direzione Generale, Guardia di Finanza ecc.), con avvertimento preventivo agli utenti interessati al controllo e nel rispetto delle regole e tutele della Privacy dettate dal Garante.

6. Utilizzo rete esterna Internet

- È fatto divieto memorizzare dalla rete documenti, file e dati 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[2], acquisti on-line e simili, salvo nei casi direttamente autorizzati dalla Direzione 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;
- La Direzione si riserva la facoltà di creare filtri idonei ad evitare navigazioni in siti non correlati all'attività lavorativa oltre che prevedere delle black-list [3].

[1] **Log di accesso**: Con il significato di *giornale di bordo*, o semplicemente *giornale*, su cui vengono registrati gli eventi in ordine cronologico il termine è stato importato nell'informatica (1963) per indicare: 1.la ***registrazione cronologica*** delle operazioni man mano che vengono eseguite, 2. il ***file*** su cui tali registrazioni sono memorizzate.
Oggi è un termine universalmente accettato con questo significato di base, con tutte le sfumature necessarie nel contesto specifico.

[2] Per **remote banking** s'intende i servizi automatizzati che consentono ai clienti di collegarsi all'elaboratore della banca presso la quale intrattengono il rapporto di conto corrente tramite terminali interattivi trasportabili o installati nei propri locali e la normale linea telefonica.
Il cliente può effettuare direttamente una serie di operazioni bancarie o ricevere informazioni in tempo reale.

[3] Una **BlackList** e' una lista di indirizzi noti come sorgenti di spam. Possono venir utilizzate per eliminare le mail nella propria mailbox. Quando un fornitore di servizi internet ospita uno spammer (colui che genera messaggi indesiderati) e non provvede alla rimozione dell'account, viene inserito nella BlackList in modo che le mail inviate da quella locazione vengano automaticamente cestinate.

7. Utilizzo posta elettronica

Le caselle di posta elettronica date in uso al dipendente sono destinate ad un utilizzo di tipo aziendale.
Si notifica 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;
- In caso di assenza, al dipendente sono posti a disposizione apposite funzioni di sistema che consentano di inviare automaticamente messaggi di risposta.
- 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.
- 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".

8. Gestione, conservazione e controllo dei dati informatici

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

9. Segreto professionale

- 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 dalla società, né potrà usarle, sfruttarle o disporne in proprio o tramite terzi.
- 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

- 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 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:
    1. 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;
    2. 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:

1. che al momento in cui vengono rese note siano di pubblico dominio;
2. 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.

11. Applicazione ed interpretazione del presente regolamento

- Per qualsiasi dubbio relativo all'applicazione pratica o all'interpretazione del presente regolamento, il dipendente può rivolgersi alla Direzione.

12. Disciplina deroghe e modifiche del presente regolamento

- Qualora vengano apposte delle modifiche al presente regolamento, 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.

Il presente regolamento verrà presentato al personale a tempo indeterminato e determinato dell'ASP e firmato per conoscenza da tutti i dipendenti dell'ASP.