REGOLAMENTO INFORMATICO INTERNO

Allegato **3** al Modello di organizzazione, gestione e controllo ai sensi del decreto legislativo 8 Giugno 2001 n° 231

In vigore dal:
10/04/2013
In sostituzione di quello in vigore dal:
31/03/2010 Rev. 3

Data approvazione:
Deliberazione del C.D.A. n. 2 del 10/04/2013

1. Utilizzo della strumentazione

1. Premesso che l'Azienda si riserva il controllo e la gestione integrale delle risorse informatiche aziendali, è fatto divieto installare sulla strumentazione in uso, hardware fisso o removibile (a titolo esemplificativo ma non esaustivo: supporti esterni, modem, ecc.) qualora ciò non risulti espressamente richiesto ed autorizzato dall'Azienda. L'utente deve pertanto utilizzare esclusivamente la strumentazione posta a disposizione dall'Azienda.
2. Il Personal Computer, i telefoni aziendali e la relativa dotazione hardware e software, affidati al dipendente costituiscono uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione, minacce alla sicurezza, nonché può generare il rischio di commissione di reati specifici. Si dispone pertanto che tutto il personale usi la massima cura nella gestione delle apparecchiature informatiche di cui è responsabile e si attenga rigorosamente alle disposizioni del presente regolamento.
3. L'Azienda si riserva di rimuovere qualsiasi elemento hardware la cui installazione non sia stata appositamente prevista o autorizzata.
4. In caso di allontanamento dalla propria postazione hardware, è fatto obbligo all'utente di attivare il salva-schermo protetto da password. Non sono ammesse condotte atte ad aggirare tale misura di sicurezza.
5. 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.
6. Qualora si rendessero necessarie modifiche alle configurazioni impostate sul PC in uso, occorre darne comunicazione al Responsabile dell'area di competenza che si attiverà per le procedure necessarie.

2. Accesso ed uso dei sistemi

1. L'utente si connette alla rete tramite autenticazione univoca personale.
2. Le credenziali di autenticazione alla rete (o se l'Utente lavora in locale, di accesso al sistema operativo) devono essere custodite e preservate dalla conoscibilità di colleghi o soggetti esterni all'Azienda.
3. A norma del Decreto Legislativo n. 196/2003, le password non devono contenere riferimenti agevolmente riconducibili all'utilizzatore. Qualora la password non corrisponda ai dettami di legge, ne risponderà penalmente e civilmente direttamente il soggetto che ne ha determinato la composizione.

4. In nessun caso devono essere annotate password in chiaro sia su supporto cartaceo che informatico.
5. 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 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.
6. Qualora l'intestatario della password ritenga che un soggetto non autorizzato possa essere venuto a conoscenza della propria password, dovrà provvedere immediatamente a comunicarlo al titolare.

3. Creazione nuova utenza o disabilitazione di utenza attiva

Qualora si renda necessaria la creazione di una nuova utenza o la disabilitazione di una utenza attiva, la richiesta potrà essere avanzata al Responsabile del settore di appartenenza dell'incaricato che provvederà nei modi convenuti all'uopo.

4. Installazione di programmi

1. Sul pc in uso non devono essere installati programmi che non siano ufficialmente forniti dalla Società. E' onere dell'Utente verificare – all'atto di entrata in vigore del presente regolamento, e periodicamente almeno ogni tre mesi – che sul pc in dotazione non siano presenti programmi in esubero rispetto a quelli indicati dal titolare; in tal caso sarà onere dell'Utente provvedere alla rimozione o segnalarlo al Responsabile dell'area di competenza che si attiverà per le procedure necessarie.
2. E' fatto divieto all'Utente sottoscrivere licenze – anche a titolo gratuito – per programmi finalizzati ad essere installati sul pc in uso del medesimo Utente.
3. L'Azienda, 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.

5. Utilizzo di supporti magnetici e dati

1. È fatto obbligo conservare e custodire all'interno dell'azienda 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/dato estraneo all'attività lavorativa o non espressamente autorizzato, non può, nemmeno in via transitoria, essere salvato sul pc in uso all'Utente.

6. Utilizzo della 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 lavorativi.
2. Qualora nella rete interna debbano circolare dati, notizie ed informazioni aziendali, deve essere premura di ciascun Utente preservare gli stessi dalla conoscibilità di terzi soggetti non espressamente autorizzati ad aver notizia di tali dati.

7. Utilizzo della rete esterna Internet

1. E' fatto divieto memorizzare dalla rete documenti, file o dati comunque non attinenti lo svolgimento delle attività aziendali, in particolare:

a) non è consentito navigare in siti non attinenti allo svolgimento delle mansioni assegnate;
b) è fatto assoluto divieto di navigare in siti, scaricare, scambiare ed utilizzare materiale pornografico o pedopornografico che possa fare incorrere nei reati di pornografia minorile (art. 600-ter codice penale) e detenzione di materiale pornografico (art. 600-quater codice penale) e così ledere all'immagine di PUBLICASA S.P.A.;
c) non è consentita l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo quanto espressamente autorizzato per la gestione ordinaria delle attività di pagamento;
d) è vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;
e) 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 l'Azienda 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.

3. Gli archivi di log risultanti da questo monitoraggio contengono traccia di ogni operazione di collegamento effettuata dall'interno della rete societaria verso Internet.
4. Eventuali attivazioni di controlli specifici saranno preventivamente comunicate; resta inteso che in caso di anomalie, l'Azienda potrà effettuare verifiche dirette a fini di monitoraggio e controllo delle risorse informatiche, che potranno incidentalmente consentire la conoscibilità dei log di connessione relativi anche ad una sola postazione. Limitando in ogni caso temporalmente il relativo controllo e la conservazione dei log di connessione.
6. E' fatto divieto all'Utente cedere il controllo del pc a server esterni (a titolo esemplificativo e non esaustivo: e-mule, peer to peer, ecc.). L'unica tolleranza prevista riguarda l'utilizzo di skype autorizzato dal titolare per comunicazioni interne tra i dipendenti afferenti l'attività aziendale.

8. Accesso ed utilizzo di banche dati esterne

1. Quando, per ragioni di lavoro, al dipendente sono assegnate, anche temporaneamente, delle credenziali per l'accesso a sistemi informativi o a banche dati esterne, questi è tenuto ad osservare le seguenti regole:
   a) È fatto divieto di cedere, comunicare o scrivere su supporti cartacei visibili a terzi le proprie credenziali personali;
   b) Le credenziali devono essere custodite con la massima diligenza e preservate dalla conoscibilità di colleghi o soggetti esterni all'Azienda.
   c) L'utilizzo dei sistemi o delle banche dati deve essere esclusivamente connesso allo svolgimento dei propri doveri di ufficio;
   d) È fatto assoluto divieto di accesso al di fuori degli orari di ufficio, tramite computer personali (se non espressamente autorizzati) ed oltre le esigenze di ufficio; ogni accesso che sarà rilevato in violazione ai presenti principi sarà considerato abusivo.
   e) È fatto divieto di danneggiare ed alterare in qualsiasi modo i sistemi o le banche dati esterne;
   f) Al momento della cessazione del rapporto di lavoro o al termine delle attività di ufficio per le quali l'accesso si era reso necessario, il dipendente è tenuto ad distruggere le credenziali di accesso, restituire eventuali supporti magnetici (tipo smart card) alla Direzione Generale.
   2. L'azienda sanziona i comportamenti in violazione alle norme comportamentali espresse nel presente paragrafo e che possono determinare una responsabilità amministrativa ai sensi del D.Lgs 231/2001 per la violazione di uno dei reati ivi previsti.

9. Utilizzo della posta elettronica

1. Le caselle di posta elettronica date in uso all'utente sono destinate ad un utilizzo di tipo esclusivamente aziendale.

Si rappresenta che:

a) 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;

f) non è consentito l'utilizzo della posta elettronica per lo scambio di materiale pornografico o pedopornografico che possa fare incorrere nei reati di pornografia minorile (art. 600-ter codice penale) e detenzione di materiale pornografico (art. 600-quater codice penale) e così ledere all'immagine di PUBLICASA S.P.A.;

b) 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.

2. In caso di assenza programmata è onere dell'Utente richiedere reindirizzamento a collega;
3. 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 gli Utenti in ottemperanza agli obblighi di fedeltà e correttezza.
4. I messaggi di posta elettronica saranno memorizzati seguendo le seguenti procedure e tempistiche: - per i messaggi in entrata, l'Utente è responsabile della selezione e conservazione degli stessi su pc dato in dotazione, in quanto la gestione avviene esclusivamente in locale; - per i messaggi in uscita, gli stessi resteranno memorizzati su server posta elettronica, con disponibilità al recupero nel caso in cui ciò si renda necessario a livello lavorativo; predetti messaggi restano memorizzati per 7 giorni.

10. Gestione, conservazione e controllo dei dati informatici

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

11. Segreto professionale

1. Al dipendente/collaboratore è fatto divieto di 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. Nella valutazione delle informazioni, il dipendente/collaboratore si impegna a prendere ogni misura perché le stesse rimangano

segrete, essendo inteso che, in caso di divulgazione non autorizzata dalla Società, sarà a carico del dipendente/collaboratore l'onere di provare di avere adottato tutta la diligente richiesta per evitare il danno conseguente.

2. Il dipendente/collaboratore rimane responsabile dei danni eventualmente subiti dalla Società in caso di violazione degli obblighi di cui alla presente clausola.
3. Gli obblighi del dipendente/collaboratore previsti in questo capo non si esauriranno con la cessazione del rapporto di lavoro/collaborazione.

12. Riservatezza dati

1. 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/collaboratore si impegna a considerare le Informazioni Riservate come strettamente private e ad adottare tutte le misure necessarie per non pregiudicare la riservatezza di tali informazioni.
2. Il dipendente/collaboratore si impegna ad utilizzare le Informazioni Riservate unicamente allo scopo di svolgere l'attività cui è preposto e di conseguenza a non usare tali informazioni in modo da arrecare danno alla Società, né per alcun altro scopo di qualsiasi natura.
3. Gli impegni di cui al presente capo non proibiscono di comunicare Informazioni Riservate:

a) ad amministratori e dipendenti, anche di enti convenzionati (Inps, Inail ed enti previdenziali), avvocati, revisori, banche o altri consulenti ai quali la conoscenza di tali Informazioni è necessaria al fine dell'espletamento di attività funzionali alla Società;
b) a soggetti diversi da quelli specificati alla precedente lettera a), qualora ciò sia stato autorizzato dalla Società;

4. L'obbligo di riservatezza non opera in caso di informazioni:

a) che al momento in cui vengono rese note siano di pubblico dominio;
b) che diventino di pubblico dominio dopo essere state rese note per causa non imputabile al dipendente/collaboratore.

5. 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.

13. Applicazione ed interpretazione del presente regolamento

1. Per qualsiasi dubbio relativo all'applicazione pratica o all'interpretazione del presente regolamento, il dipendente/collaboratore può rivolgersi al proprio responsabile.

14. Disciplina deroghe e modifiche del presente regolamento

1. Qualora al presente regolamento la Società intenda apporre modifiche, queste saranno applicate dandone conoscenza immediata al dipendente/collaboratore.
2. Deroghe o modifiche di una o più clausole del presente regolamento non comportano la sua integrale modifica o quelle non direttamente emendate, salva l'ipotesi di evidente incompatibilità.

15. Responsabilità

1. La violazione di una qualsiasi delle clausole di cui al presente regolamento, dà diritto alla Società di procedere disciplinarmente nei confronti del dipendente/collaboratore infedele.
2. La Società altresì sanziona i comportamenti in violazione alle norme comportamentali espresse nel presente paragrafo che possono determinare una responsabilità amministrativa ai sensi del D.Lgs 231/2001 per la commissione di uno dei reati ivi previsti.
3. Qualora la Società venga a conoscenza di una violazione del presente regolamento che costituisca illecito civile o penale, provvederà immediatamente a darne avviso alla competente Autorità.

16. Applicazione ed interpretazione del presente regolamento

1. Per qualsiasi dubbio relativo all'applicazione pratica o all'interpretazione del presente regolamento, l'Utente può rivolgersi al suo diretto responsabile.

17. Disciplina deroghe e modifiche del presente regolamento

1. Qualora al presente regolamento l'Azienda intenda apporre modifiche, queste saranno applicate dandone conoscenza.
2. Deroghe o modifiche di uno o più punti del presente regolamento, non rendono invalidi gli altri punti.
3. Eventuali violazioni di una delle clausole ivi contenute, può comportare l'adozione di un provvedimento di tipo disciplinare.