EDILIZIA RESIDENZIALE PUBBLICA MASSA CARRARA S.P.A.

REGOLAMENTO INFORMATICO AZIENDALE

Regolamento Aziendale per la sicurezza e l'utilizzo della postazione di informatica individuale

(Approvato dal C. di A. il 12/04/2012 delibera n. 30)

Indice:

Premessa

1. Utilizzo del Personal Computer
2. Utilizzo della rete
3. Gestione delle Password
4. Utilizzo dei PC portatili
5. Uso della posta elettronica
6. Uso della rete Internet e dei relativi servizi
7. Protezione antivirus
8. Osservanza delle disposizioni in materia di Privacy
9. Non osservanza della normativa societaria e relativi provvedimenti disciplinari
10. Aggiornamento e revisione

Premessa

La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete Internet dai Personal Computer, espone ai rischi di un coinvolgimento sia patrimoniale che penale, creando problemi alla sicurezza e all'immagine della Società stessa.

Premesso che l'utilizzo delle risorse informatiche e telematiche societarie deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente sono basilari in un rapporto di lavoro, ha adottato il presente regolamento, promosso dall'Amministratore di Sistema, alla luce del "Piano programmatico Societario sulla sicurezza informatica", per contribuire alla massima diffusione della cultura della sicurezza ed evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.

Il Regolamento Informatico Aziendale di seguito riportato viene incontro quindi alla necessità di disciplinare le condizioni per il corretto utilizzo degli strumenti informatici da parte dei dipendenti e contiene informazioni utili per comprendere cosa può fare ogni dipendente per contribuire a garantire la sicurezza informatica di tutta la Società.

Tale prescrizione si aggiunge e integra le norme già previste dal contratto di lavoro nonché dal "Piano programmatico sulla sicurezza informatica" adottato dalla Società EDILIZIA RESIDENZIALE PUBBLICA DI MASSA E CARRARA S.p.A., denominata d'ora in avanti per praticità: E.R.P. MS S.p.A.

1 - Utilizzo del Personal Computer:

1.1 Il Personal Computer affidato al dipendente/operatore, è uno strumento di lavoro e 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.

1.2 Non è consentita l'attivazione della password d'accensione (bios), senza preventiva autorizzazione da parte dell' E.R.P. MS S.p.A.

1.3 Non è autorizzato/consentito all'operatore modificare le caratteristiche hardware e software impostate sul proprio PC, salvo previa autorizzazione esplicita da parte dell'Amministratore di Sistema della Società che per praticità d'ora in avanti sarà denominato: A. di S ..

1.4 Il Personal Computer deve essere spento ogni giorno prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio (pausa pranzo - sopralluoghi tecnici/amministrativi ecc.).

1.5 Le informazioni archiviate informaticamente devono essere esclusivamente quelle previste dalla legge o necessarie all'attività lavorativa.

1.6 Costituisce buona regola la pulizia periodica (almeno ogni sei mesi) degli archivi, con cancellazione dei file obsoleti o inutili (es. .tmp). Particolare attenzione deve essere prestata alla duplicazione dei dati. E' infatti assolutamente da evitare un'archiviazione ridondante.

1.7 La tutela della gestione locale di dati su stazioni di lavoro personali - personal computer che gestiscono localmente documenti e/o dati - è demandata all'operatore finale che dovrà effettuare, con frequenza opportuna, i salvataggi su supporti magnetici e/o di rete e la conservazione degli stessi in luogo idoneo e sicuro. E' comunque vietato l'uso di supporti di archiviazione removibili per la memorizzazione dei dati sensibili, se non opportunamente custoditi e opportunamente protetti.

1.8 Le gestioni locali dei dati nei singoli PC, dovranno essere custodite con opportuna cautela e riservatezza dagli operatori ed integrate o completamente sostituite da gestioni centralizzate su server protetti.

1.9 Non è consentita l'installazione di programmi diversi da quelli autorizzati dal Sistema Informatico dell'E.R.P. MS S.p.A. (Allegato A - Sistema Informatico E.R.P. MS S.p.A. - Elenco programmi software).

1.10 Non è consentita la riproduzione o la duplicazione di programmi informatici ai sensi della Legge n.128 del 21.05.2004.

1.11 Gli operatori autorizzati all'utilizzo del Sistema Informatico possono in qualunque momento procedere alla rimozione di ogni file o applicazione che riterranno essere pericolosi per la sicurezza sia sui propri PC sia sulle unità di rete e nel dubbio consultare l'A. di S ..

2 - Utilizzo della rete dell' E.R.P. MS S.p.A.:

2.1 L'accesso alla rete aziendale è protetto da password; per l'accesso deve essere utilizzato il proprio profilo personale (username e password).

2.2 E' fatto divieto di utilizzare la rete aziendale per fini non espressamente autorizzati.

2.3 E' vietato connettere in rete stazioni di lavoro non di proprietà della Società (PC, periferiche ecc.) se non dietro esplicita e formale autorizzazione dell'A. di S ..

2.4 E' vietato condividere cartelle in rete sia dotate di password, sia sprovviste di password se non dietro esplicita e formale autorizzazione dell'A. di S. della Società.

2.5 E' vietato monitorare ciò che transita in rete [log d'accesso 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 all'A. di S. da parte delle Autorità autorizzate ai controlli (Es. Titolare Societario, Guardia di Finanza ecc.), con avvertimento preventivo agli utenti interessati al controllo e nel rispetto delle regole e tutele della Privacy dettate dal Garante.

2.6 E' vietata l'installazione non autorizzata di modem che sfruttino il sistema di comunicazione telefonico per l'accesso a banche dati esterne o interne alla Società.

3 – Gestione delle Password:

3.1 Le credenziali d'ingresso alla rete, di accesso ai vari programmi in rete per i trattamenti dei dati e ad Internet, sono attribuite dall' A. di S. della Società.

3.2 L'operatore è tenuto a conservare nella massima segretezza la parola/codice di accesso alla rete ed ai sistemi e qualsiasi altra informazione legata al processo di autenticazione.

3.3 L'operatore è tenuto a scollegarsi dal sistema ogni qualvolta sia costretto ad assentarsi dal locale nel quale è ubicata la stazione di lavoro o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima: lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.

3.4 La password deve essere immediatamente sostituita, dando ne comunicazione all'A. di S. della Società, nel caso si sospetti che la stessa abbia perso la segretezza.

3.5 In caso di prolungata assenza (almeno una settimana) dell'operatore e per urgenze/necessità operative, è necessario rilasciare all'Amministratore di Sistema, le credenziali d'accesso al computer di pertinenza. Sarà cura dell' A. di S. comunicare tali credenziali a colui/coloro che dovranno accedere al computer del dipendente assente, registrandone gli accessi. Resta inteso che l'utilizzo del computer dell'operatore assente, deve essere limitato nel tempo ed esclusivamente ad esigenze operative aziendali (es. file, documenti, procedure, programmi ecc. che si trovano solo in quel computer), poiché per la Privacy, si tratta comunque di uno strumento di lavoro personale. Nel caso l'operatore non abbia la possibilità di comunicare le credenziali, sarà lo stesso Amministratore di Sistema a crearne di nuove per poter accedere al computer, ripristinando le originali al rientro dell'operatore interessato.

4 – Utilizzo di PC portatili:

4.1 L'utente è responsabile del PC portatile assegnatogli dalla Società e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

4.2 Ai PC portatili si applicano le regole di utilizzo previste per i PC connessi in rete con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso, prima della eventuale riconsegna all'A. di S ..

4.3 I PC portatili utilizzati all'esterno (convegni, rilevamenti tecnici ecc.), in caso di allontanamento, devono essere custoditi in un luogo protetto e sicuro.

4.4 Il portatile non deve essere mai lasciato incustodito (in caso di utilizzo all'interno della Società) e sul disco devono essere conservati solo i files strettamente necessari.

4.5 Nel caso di accesso alla rete aziendale tramite R.A.S (Remote Access Server) Accesso Remoto: utilizzare l'accesso in forma esclusivamente personale con username e password in modo rigoroso e specifici per il PC portatile.

4.6 Disconnettersi dal sistema R.A.S. al termine della sessione di lavoro.

4.7 Collegarsi periodicamente (almeno una volta a settimana) alla rete interna per consentire il caricamento dell'aggiornamento dell'anti virus.

5 – Uso della posta elettronica:

5.1 L'abilitazione alla posta elettronica deve essere preceduta da regolare richiesta del Responsabile di funzione/unità organizzativa all'A. di S ..
5.2 La casella di posta, assegnata dalla Società all'utente, è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse (art. 615 comma 5 e segg. c.p.).

5.3 Nel caso di mittenti sconosciuti o messaggi insoliti, per non correre il rischio di essere infettati da virus occorrerà cancellare i messaggi senza aprirli e nel dubbio informare l'A. di S ..

5.4 Nel caso di messaggi provenienti da mittenti conosciuti ma che contengono allegati sospetti (file con estensione .exe .scr .pif .bat .cmd), questi ultimi non devono essere aperti.

5.5 Evitare che la diffusione incontrollata di "Catene di Sant'Antonio" (messaggi a diffusione capillare e moltiplicata) limiti l'efficienza del sistema di posta.

5.6 Utilizzare, nel caso di invio di allegati pesanti, i formati compressi (*.zip; *.rar; *.jpg).

5.7 Nel caso in cui si debba inviare un documento all'esterno della Società è preferibile utilizzare un formato protetto da scrittura (ad esempio il formato Acrobat * .pdf). Il Software specifico, se non già installato nel PC è fornito dall' A. di S. previa richiesta.

5.8 L'iscrizione a "mailing list" esterne è concessa solo per motivi professionali, prima di iscriversi occorre verificare in anticipo se il sito è affidabile.

5.9 La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

5.10 Per la trasmissione di file all'interno dell'E.R.P. MS S.p.A. è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati che non devono mai superare i 4 MB.

5.11 E' obbligatorio controllare i File "attachements" (allegati) di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o ftp non conosciuti).

6 – Uso della rete Internet e dei relativi servizi:

6.1 L'abilitazione alla posta esterna e ad Internet deve essere preceduta da regolare richiesta del Responsabile di funzione/unità organizzativa, all'A. di S. della Società.

6.2 Ogni PC abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa.

6.3 E' assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.

6.4 Non possono essere utilizzati modem privati per il collegamento alla rete.

6.5 E' fatto divieto all'operatore, lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dall' E.R.P. MS S.p.A. e dal suo A. di S ..

6.6 E' vietata la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (nicknames).

7 – Protezione antivirus:

7.1 Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo (ad esempio non aprire mail o relativi allegati sospetti, non navigare su siti non professionali ecc ..) .

7.2 Ogni operatore è tenuto a controllare la presenza e il regolare funzionamento del software antivirus aziendale.

7.3 Nel caso che il software antivirus rilevi la presenza di un virus che non è riuscito a ripulire, l'utente dovrà immediatamente: sospendere ogni elaborazione in corso senza spegnere il computer e segnalare l'accaduto all'A. di S. della società.

7.4 Ogni dispositivo magnetico di provenienza esterna alla società (CD, DVD, pen drive ecc.), dovrà prima del loro utilizzo, essere verificati mediante il programma antivirus (in dotazione su ogni PC) e nel caso venga rilevato un virus non elimina bile dal software, non dovrà essere utilizzato.

8 – Osservanza delle disposizioni in materia di Privacy:

8.1 E' obbligatorio attenersi alle disposizioni di cui al Regolamento sulle misure minime di sicurezza (Regolamento Aziendale) e al Documento di Programmazione e Sicurezza di cui al contratto di lavoro della Società.

9 – Non osservanza della normativa societaria e relativi provvedimenti disciplinari:

9.1 Il mancato rispetto o la violazione delle regole contenute nel presente regolamento é perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali previste dalle leggi (art. 171-ter – art. 248/00 art. 547 - art.594 e 595 - art. 600-ter e seg. – art. 615 ter - art. 615 quater- art. 615 - quinques - art. 617 quater - art. 617 quinquies - art. 617 sexies - art. 635-bis - art. 640 e 640 ter). Ma in particolare, le regole di base in materia di obblighi e garanzie per i provvedimenti disciplinari sono dettati dall’art. 7 dello Statuto dei lavoratori (legge 300 del 1970). Le sanzioni previste (in ordine di gravità) sono: Rimprovero verbale; Rimprovero scritto; multa (fino ad un massimo di 4 ore di retribuzione); Sospensione dal servizio e dalla retribuzione per un periodo non superiore ai 10 giorni; Trasferimento, se previsto dal Ccnl e con mansioni equivalenti alle precedenti; Licenziamento.

10 – Aggiornamento e revisione:

10.1 Tutti gli operatori possono proporre, quando ritenuto necessario, integrazioni e modifiche al presente regolamento tramite comunicazione all'Amministratore di Sistema.

10.2 Il presente Regolamento Informatico Aziendale è soggetto a revisione con frequenza annuale.

L'Amministratore di Sistema
Sig. Antonio Pisanelli

Il Presidente E.R.P. MS S.p.A.
Dott. Luca Panfietti

Carrara, lì 12/04/2012