Allegato alla delibera C.C. n.8 del 29.09.2011.

COMUNE DI ROGHUDI

Prov. Reggio Calabria

REGOLAMENTO PER LA SICUREZZA E UTILIZZO DELLE POSTAZIONI DI INFORMATICA INDIVIDUALE

ART.1 -UTILIZZO DEL PERSONAL COMPUTER-

1. ***Il 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 è vietato in quanto può contribuire ad innescare disservizi, costi di manutenzione, e soprattutto, minacce alla sicurezza.***
2. ***Non è consentito all'utente modificare le caratteristiche hardware e software impostate sul proprio CP, salvo previa autorizzazione esplicita da parte del responsabile Comunale.***
3. ***Il Personale Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio.***
4. ***Le informazioni archiviate informaticamente devono essere esclusivamente quelle previste dalla legge o necessarie all'attività lavorativa.***
5. ***Costituisce buona regola la pulizia periodica (almeno ogni anno) degli archivi, con cancellazione dei file obsoleti o inutili (TMP). Particolare attenzione deve essere prestata alla duplicazione dei dati. E' infatti assolutamente da evitare un'archiviazione ridondante.***
6. ***L'utente dovrà effettuare, con frequenza opportuna, i salvataggi su supporti magnetici e/o di rete e la conservazione degli stessi in luogo idoneo. E' comunque vietato l'uso di supporti di archiviazione removibili per la memorizzazione dei dati sensibili.***
7. ***Non è consentita l'installazione di programmi diversi da quelli previsti dalla vigente normativa ovvero autorizzati..***
8. ***Non è consentita la riproduzione o la duplicazione di programmi informatici ai sensi delle leggi n. 128 del 21.05.2004.***

ART.2 Utilizzo della rete e del sistema informatico.

1. ***L'accesso alla rete nonchè al sistema informatico è protetto da password che è strettamente personale.***
2. ***E' fatto divieto di utilizzare la rete informatica per fini personali.***

ART:Gestione della password.

1. ***L'utente è tenuto a conservare nella massima segretezza la parola di accesso alla rete ed ai sistemi informatici e qualsiasi altra informazione legata al processo di autenticazione.***
2. ***L'utente 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.***

ART.4 Utilizzo dei PC portatili.

1. *L'utente è responsabile del PC portatile assegnatogli dal Comune e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo del luogo di lavoro.*

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 riconsegna.*
3. *I PC utilizzati all'esterno (convegni, visite in azienda) in caso di allontanamento, devono essere custoditi in luogo protetto.*
4. *Il portatile non deve essere mai lasciato incustodito e sul disco devono essere conservati solo i file strettamente necessari.*
5. *Nel caso di accesso alla rete aziendale tramite RAS (remote Access Server) Accesso Remoto: utilizzare l'accesso in forma esclusivamente personale utilizzare la password in modo rigoroso. Disconnettersi dal sistema RAS al termine della sessione di lavoro.*
6. *Collegarsi periodicamente alla rete interna per consentire il caricamento dell'aggiornamento dell'antivirus.*
7. *Non utilizzare abbonamenti Internet per collegarsi in rete.*

ART.5 Uso della posta elettronica.

1. *Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo del corretto utilizzo delle stesse (art. 615 comma 5 e segg. c.p.) e dell'uso della password personale.*
2. *Nel caso di mittenti sconosciuti o messaggi insoliti, per non correre il rischio di essere infettati da virus occorrerà cancellare i messaggi senza aprirli.*
3. *Nel caso di messaggi provenienti da mittenti sconosciuti ma che contengono allegati sospetti (file con estenzione exe.scr. pif. Bat. cmd) questi ultimi non devono essere aperti.*
4. *Evitare che la diffusione incontrollata di "Catene di Sant'Antonio " (messaggi a diffusione capillare e moltiplicata) limiti l'efficienza del sistema di posta.*
5. *L'utilizzare, nel caso di invio di allegati pesanti, i formati compressi (* zip *rar.*jpg)*
6. *La casella di posta deve essere mantenuta in ordine cancellando documenti inutili e soprattutto allegati ingombranti.*

ART.6 Uso della rete Internet e dei relativi servizi.

1. *L'abilitazione alla posta esterna e ad Internet deve essere preceduta da regolare autorizzazione. Il PC abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa.*
2. *E' assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.*
3. *Non possono essere utilizzati modem privati per il collegamento alla rete.*
4. *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 pseudomini (o nicknames).*

ART.7 Protezione antivirus.

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.)*
2. *Ogni utente è tenuto a controllare la presenza e il regolare funzionamento del software antivirus comunale.*
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- segnalare l'accaduto al responsabile per la sicurezza del Comune.

4. ***Ogni dispositivo magnetico di provenienza esterna all'azienda dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus non eliminabile dal software, non dovrà essere utilizzato.***

ART.8 Osservanza delle disposizioni in materia di Privacy.

1. ***E' obbligatorio attenersi alle disposizione in materia di Privacy di cui alla vigente normativa ed inoltre al Documento di Programmazione e Sicurezza.***

ART.9 Non osservanza della normativa aziendale.

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

ART.10 Norme finali.

1 . Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente regolamento.

2. ***Il presente Regolamento è soggetto a revisione con frequenza triennale.***

3. Ulteriori aspetti di dettaglio in merito alla sicurezza e utilizzo delle postazioni di informatica individuale verranno disciplinati con disposizione del Sindaco.