REGOLAMENTO PER L'ACCESSO AL SERVIZIO INTERNET DA PARTE DEGLI UFFICI COMUNALI E PER L'UTILIZZO DELLE POSTAZIONI INFORMATICHE.

Art. 1 - Finalità del regolamento

Il regolamento intende disciplinare l'accesso e l'utilizzo degli strumenti informativi di Internet da parte dei dipendenti del Comune di Solesino.

Art. 2 - Punti di accesso

I punti di accesso ad Internet, messi a disposizione del dipendente pubblico e sottoposti a regolamentazione sono i personal computer preventivamente predisposti nella configurazione da parte del responsabile del 5^ Settore "Uso ed assetto del territorio".

Art. 3 - Orari

L'accesso alla rete internet sarà attivo nel rispetto degli orari stabiliti dai rispettivi responsabili di settore in base alle esigenze del servizio esplicato degli uffici competenti e comunque durante il normale orario di servizio.

Art. 4 - Utenza

Possono usufruire degli accessi Internet tutti i dipendenti preventivamente autorizzati dal proprio responsabile di settore, con comunicazione scritta da effettuarsi al Responsabile del 5^ Settore "Uso ed assetto del territorio", di cui all'art. 2, indicante il tipo di accesso da abilitare che precisi rispettivamente:

- orario di abilitazione;
- tipo di accessibilità : totale o parziale con eventuale elenco degli indirizzi URL (siti) che saranno disponibili per l'accesso;
- durata autorizzazione (temporanea,limitata ad un periodo o continuativa);

Art. 5 - Utilizzo delle postazioni con accesso alla rete Internet

Le stazioni abilitate all'accesso ad Internet dovranno essere, utilizzate per attività di supporto alle proprie mansioni lavorative che richiedano l'ausilio di strumenti telematici e/o multimediali.
Tali attività dovranno essere congruenti con la natura, le finalità e gli scopi dei soggetti di cui all'art. 4.
L'accesso alla rete Internet non può essere utilizzato per scopi commerciali e/o di lucro, per attività illegali, e per scopi personali.
Inoltre è vietato manomettere e/o modificare il Software e l'Hardware in dotazione e/o installare ex novo componenti hardware e software da parte dell'utenza.. Nel caso in cui per una completa e corretta gestione della propria attività lavorativa sia necessario installare software (ad esempio software dell'Agenzia delle Entrate del Ministero dell'Interno) è necessario concordarlo preventivamene con il Responsabile del 5^ Settore "Uso ed assetto del territorio"

Art. 6 - Responsabilità degli utenti

Ogni utente è responsabile e come tale dovrà rispondere per l'eventuale inosservanza delle norme contenute nel presente regolamento.

Art. 7 – Regole operative e operazioni di verifica e controllo

Non è consentito agli utenti abilitati all'accesso ad Internet di eseguire il download (scarico di programmi e/o

files) di software o di file musicali e/o multimediali (video,musica etc)
Non è consentito in ogni caso l'utilizzo di indirizzi e-mail personali in software di posta elettronica locali (Outlook, Thunderbird, Incredimail etc).
E' consentito utilizzare anche per ragioni personali servizi di posta elettronica ricorrendo a sistemi di consultazione o invio detti 'webmail', previa comunicazione al Responsabile del 5^ Settore "Uso ed assetto del territorio", indicandone le modalità e l'arco temporale di utilizzo (ad esempio fuori dall'orario di lavoro o durante le pause etc). Gli accessi alla rete sono memorizzati in file di log, che contengono in formato testuale i seguenti dati relativi al collegamento alla rete internet:

- Indirizzo IP
- Link pagina web visitata
- Link download eseguiti
- Tempo di collegamento

Con frequenza bimestrale l'Ente attraverso il Segretario Generale si riserva di effettuare controlli in conformità alla legge, al fine di verificare il rispetto di tutte le regole di accesso alla rete internet al fine di garantire funzionalità e sicurezza del sistema.

Il riscontro delle eventuali violazioni delle regole di accesso alla rete internet vengono comunicati ai Responsabili di Servizio per i provvedimenti di competenza.

L'accesso e la consultazione dei file di log è possibile solo dall'interno della rete e solo da parte del Segretario Generale.

Tali file di log sono conservati per un periodo pari a mesi 6 (sei);

Art. 8 - Revoca accessi

A fronte di accertate violazioni del regolamento, i Responsabili di Settore degli uffici preposti alle singole postazioni Internet hanno facoltà, con provvedimenti motivati, di revocare temporaneamente o definitivamente l'accesso dei soggetti di cui all'art. 4 con contestuale comunicazione scritta al Responsabile del 5^ Settore "Uso ed assetto del territorio" ed al Segretario Generale.
Gli stessi responsabili di servizio a fronte di danni accertati provocati da inosservanza delle presenti norme, avviano le eventuali procedure disciplinari di rivalsa economica.

Art. 9 - Regole per la sicurezza e l'utilizzo delle postazioni di informatica individuale

Utilizzo del Personal Computer

Il Personal Computer affidato al dipendente è uno strumento di lavoro di cui 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.

Non è consentita l'attivazione della password d'accensione (bios), senza preventiva autorizzazione da parte del Responsabile del 5^ Settore "Uso ed assetto del territorio".

Non è consentito all'utente modificare le caratteristiche hardware e software impostate sul proprio PC, se non previa autorizzazione esplicita da parte del Responsabile del 5^ Settore "Uso ed assetto del territorio".

Il Personal Computer ed il relativo gruppo di continuità (se presente) devono essere spenti ogni giorno prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio.

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

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

da evitare un'archiviazione ridondante.

La tutela della gestione locale di dati su stazioni di lavoro personali – personal computer che gestiscono localmente documenti e/o dati - è demandata all'utente finale che dovrà effettuare, con frequenza opportuna, i salvataggi su server preposto ed indicato da parte del personale del 5^ Settore "Uso ed assetto del territorio".

E' vietato l'uso di supporti di archiviazione removibili per la memorizzazione dei dati sensibili.

Non è consentita l'installazione di programmi diversi da quelli autorizzati dal Sistema Informativo Comunale se non previa autorizzazione del responsabile dell'Unità Informativa.

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

Il Responsabile del 5^ Settore "Uso ed assetto del territorio" può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterranno essere pericolosi per la sicurezza sia sui personal computers degli incaricati sia sulle unità di rete.

In caso di prolungata assenza dell'utente il Responsabile del 5^ Settore "uso ed assetto del territorio" è autorizzato a sostituire la password di accesso al personal computer al fine di garantire la possibilità di prelevare files che siano necessari alla prosecuzione dell'attività lavorativa dell'Ente.

Gestione delle Password

Le password di accesso al dominio di rete, alla rete internet ed ai vari programmi in rete per i trattamenti dei dati, sono attribuite dal Responsabile del 5^ Settore "Uso ed assetto del territorio".

L'utente è tenuto a conservare nella massima segretezza le passwords di accesso alla rete ed ai sistemi informativi oltre a qualsiasi altra informazione legata al processo di autenticazione.

L'utente è tenuto a scollegarsi dal sistema informativo (esempio dalle procedure gestionali kibernetes) o attivare uno screen-saver 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, infatti 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.

Uso della posta elettronica

L'abilitazione alla posta elettronica esterna deve essere preceduta da regolare richiesta da parte del proprio responsabile del settore, con comunicazione scritta da effettuarsi al Responsabile del 5^ Settore "Uso ed assetto del territorio", la casella di posta, assegnata dall'Ente 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.).

Nel caso di mittenti sconosciuti o messaggi insoliti, per non correre il rischio di essere infettati da virus occorrerà cancellare i messaggi senza aprirli.

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.

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

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

Nel caso in cui si debba inviare un documento all'esterno dell'Ente è preferibile utilizzare un formato protetto da scrittura (ad esempio il formato Acrobat *.pdf). Tale software specifico è fornito dal personale del 5^ Settore "Uso ed assetto del territorio", previa richiesta.

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

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

Protezione antivirus

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

Ogni utente è tenuto a controllare la presenza e il regolare funzionamento del software antivirus installato e 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 al personale del 5^ Settore "Uso ed assetto del territorio".

Ogni dispositivo informatico di provenienza esterna all'Ente (CD ROM /DVD /Penne USB etc) 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.

Osservanza delle disposizioni in materia di Privacy

E' obbligatorio attenersi alle disposizioni sulle misure minime di sicurezza previste per Legge oltre a quelle contenute nel Documento di Programmazione e sicurezza annualmente approvato dall'Ente.
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 - Aggiornamento e revisioni

Tutti gli utenti possono proporre tramite i rispettivi Responsabile di Settore, quando ritenuto necessario, integrazioni al presente regolamento, a mezzo comunicazione scritta al Responsabile del 5^ Settore "Uso ed assetto del territorio":
Il presente Regolamento è soggetto a revisione almeno con frequenza triennale.