COMUNE DI MARCON
Provincia di Venezia

REGOLAMENTO PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI E DI INTERNET

(Norme di sicurezza conformi alla
normativa vigente in tema di trattamento dei dati personali, tutela
del diritto d'autore, criminalità informatica e alle migliori prassi in uso).

Approvato con delibera di Giunta Comunale n. 206 del 06.09.2007

Art. 1: Oggetto e finalità
L'utilizzo di strumentazione informatiche e di internet costituisce un importante strumento per la realizzazione di una attività amministrativa che attui i principi di buon andamento, efficacia ed efficienza dei procedimenti, in conformità alla L. 241/90, al D. Lgs. 267/2000 e al D.Lgs. 165/2001.
La regolamentazione che segue ha l'intento di:

- garantire la massima efficienza delle risorse informatiche e del loro utilizzo;
- garantire la riservatezza delle informazioni e dei dati;
- provvedere ad un servizio continuativo nell'interesse dell'Ente;
- garantire il rispetto delle leggi in materia di utilizzo delle risorse informatiche;
- garantire la massima sicurezza nell'interazione tra il comune di Marcon e altre istituzioni.

il tutto tenendo conto delle disposizioni della vigente normativa in tema di trattamento dei dati personale e relative misure minime di sicurezza (artt. 33-36 e allegato B, D.Lgs 196/2003).

Art. 2: Definizioni
Per *risorse informatiche* si intendono:

- *workstation*, personal computer fissi o portatili, stampanti locali o di rete, palmari, utilizzati da dipendenti, amministratori, collaboratori, stagisti, tirocinanti, ospiti e utilizzatori dei servizi offerti dal comune (biblioteca, sala informatica, ecc.);
- tutte le macchine facenti comunque parte della rete del comune di Marcon;
- apparati di rete;
- tutto il software e i dati acquisiti o prodotti per l'amministrazione dei sistemi, per l'utilizzo da parte degli utenti o di terzi autorizzati.

Il presente regolamento è rivolto agli utilizzatori delle risorse informatiche, ovvero: dipendenti, amministratori, collaboratori, stagisti, tirocinanti ed eventuali ospiti e utilizzatori dei servizi offerti dal comune (di seguito chiamati utenti).

Art. 3: Modalità di utilizzo delle risorse informatiche
Ogni utente deve custodire la propria strumentazione in modo appropriato e diligente, segnalando tempestivamente ogni danneggiamento, furto o smarrimento al proprio responsabile e al personale addetto ai sistemi informatici verbalmente e tramite posta interna.

L'utilizzo degli strumenti informatici al di fuori dell'orario di servizio è consentito solo previa autorizzazione del proprio responsabile.

Ogni utente è tenuto ad osservare le direttive del personale addetto ai sistemi informatici volte a garantire il corretto funzionamento delle procedure di backup.

I dati, documenti o file di qualsiasi genere (creati o modificati attraverso le applicazioni di produttività individuale - es. office o open-office-) devono essere salvati solo sui supporti appositamente destinati sul Server (unità di rete con cartelle dedicate agli uffici: \\Server2000\Marcon).
Tale disposizione può essere derogata, su disposizione del responsabile di settore, solo per motivi tecnici.

Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono, in alcun modo, essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, neppure per brevi periodi, in queste aree.

Durante le sessioni di lavoro gli strumenti elettronici non possono essere lasciati incustoditi e accessibili a terzi. Pertanto, ogni qualvolta l'utente si allontani o si assenti dalla postazione di lavoro usata per il trattamento dei dati, è tenuto a chiudere la sessione, oppure a rendere inaccessibile a terzi (ad esempio mediante l'utilizzo del salvaschermo dotato di password) la propria postazione di lavoro. [regola allegato B punto 9 del D.Lgs. 196/2003]

Si possono effettuare copie di dati su supporti rimovibili (es. dischetti CD, DVD, chiavi usb) solo se autorizzati da parte del capo settore. Qualora sulle copie venissero trasferiti dati personali, gli stessi vanno utilizzati con le modalità previste dalla legge, e secondo principio di necessità. Al termine del trattamento sarà cura dell'utente rimuovere i dati personali dai supporti stessi.

Dai supporti rimovibili contenenti dati sensibili o giudiziari, se non utilizzati, devono essere rimossi i dati e possono essere riutilizzati da altri utenti, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e in alcun modo ricostruibili.

Per rispetto delle norme che regolano la tutela giuridica del software e per la necessità di garantire integrità e stabilità delle applicazioni installate sul personal computer stesso non è consentito:

1. alterare, rimuovere o danneggiare le configurazioni del software e dell'hardware dei personal computer ;
2. installare e utilizzare programmi informatici che non siano stati ufficialmente forniti o acquistati dal Comune;
3. installare giochi, screensavers, client chat etc;
4. installare dispositivi di comunicazione (*modem*) se non con l'autorizzazione espressa del responsabile dei Sistemi informatici;
5. installare o connettere periferiche proprie;
6. scaricare da internet o da supporto magnetico proveniente dall'esterno file di provenienza sconosciuta senza farli sottoporre a opportuno controllo;
7. divulgare informazioni tecniche relative alla struttura informatica comunale che possano pregiudicare la sicurezza della stessa;
8. utilizzare strumenti software e/o hardware atti a interpretare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici.

E' inoltre espressamente vietato:

1. utilizzare gli strumenti informatici comunali al fine di custodire, far circolare o promuovere materiale pubblicitario personale, codice maligno *(virus, trojan horses, programmi pirata)* o altre porzioni di codice maligno e/o altro materiale non autorizzato.
2. copiare o mettere a disposizione di altri materiale protetto dalla legge sul diritto d'autore (documenti, *files* musicali, immagini, filmati e simili) di cui l'ente non abbia acquisito i diritti.
3. utilizzare la strumentazione informatica per la realizzazione, redazione, memorizzazione e spedizione di documenti di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione, appartenenza sindacale e politica.

Tutti i file di provenienza esterna e certa, attinenti all'attività lavorativa, prima di essere aperti devono essere scansionati utilizzando gli appositi programmi (antivirus) installati nel proprio personal computer.

Il personale addetto ai sistemi informatici qualora verificasse, anche a seguito dei normali interventi tecnici sul computer dell'utente o sulle risorse di rete, il mancato rispetto delle regole del presente regolamento, dovrà riferire per iscritto al segretario generale, al responsabile del settore del dipendente e al responsabile dei sistemi informatici. La comunicazione dovrà illustrare le violazioni registrate e gli interventi necessari per ripristinare la situazione iniziale.

Art. 4: Autenticazione Informatica
Il trattamento di dati personali sul computer comunale è consentito, all'interno dell'ente, solamente agli incaricati dotati di personali credenziali di autenticazione ovvero del codice per l'identificazione dell'utente (user id) associato a una parola chiave (password). [reg. B1 e 2]

La parola chiave è riservata, deve essere conosciuta solamente dall'utente che non deve, in alcun caso, comunicarla a terzi. [reg. B2]

Ogni dispositivo hardware di autenticazione (chiave hardware) deve rimanere in possesso e uso esclusivo dell'utente. Il dispositivo è di proprietà dell'ente, non può essere né prestato né ceduto a terzi, neppure temporaneamente. In caso di allontanamento, anche solo temporaneo, dall'elaboratore, il dispositivo deve essere estratto e custodito. [reg. B2 e 4]

La parola chiave deve essere composta da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili al dipendente. [reg. B5]

Le credenziali e la password sono attribuite unicamente dal personale autorizzato dal Comune e le stesse possono essere assegnate unicamente al personale autorizzato. La parola chiave deve essere modificata dal dipendente al primo utilizzo e, successivamente, almeno ogni sei mesi (ogni tre mesi nel caso di trattamento di dati sensibili). A tal fine il personale addetto ai sistemi informatici adotta le misure tecniche necessarie affinché la procedure di modifica della parola chiave venga proposta automaticamente all'utente [reg. B5]. Dopo la prima modifica la parola chiave deve essere conosciuta solamente dall'utente che non deve, in alcun caso, comunicarla a terzi.

In caso di assenza del dipendente, e contingente necessità indispensabile e indifferibile di intervenire per esclusive necessità di operatività e di sicurezza del sistema, il responsabile del servizio può assicurare la disponibilità di dati e degli strumenti informatici richiedendo al responsabile dei sistemi informatici l'attribuzione di nuove credenziali di accesso ed eventuale assegnazione delle credenziali ad un nuovo temporaneo incaricato sostitutivo. Al suo ritorno, il dipendente verrà informato dal responsabile del settore di appartenenza tempestivamente circa l'intervento effettuato. [reg. B10]

Il personale addetto ai sistemi informatici adotta le misure, prioritariamente tecniche, affinché [reg. B6,7 e 8]:

- il codice di autenticazione non possa essere assegnato ad altri incaricati, neppure in tempi diversi;
- le credenziali di autenticazione non utilizzate da almeno sei mesi siano disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
- Le credenziali siano disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

Art. 5: Rischio di Intrusione e *Antivirus*
Al fine di proteggere i dati dal rischio di accesso abusivo e dall'azione dannosa di programmi (ad esempio v*irus),* l'ente predispone a livello centralizzato, adeguati strumenti elettronici nonché il loro aggiornamento secondo le modalità previste dalla legge. [reg. B16-17]
Il personale è tenuto a segnalare ogni malfunzionamento degli strumenti programmi antivirus, ed affini e per nessun motivo è autorizzato a disattivarli*.*

Art. 6: Navigazione Su Internet e Relativi Servizi

La rete Internet è una risorsa messa a disposizione del personale come fonte di informazione per finalità di documentazione, ricerca e studio utili per lo svolgimento del proprio lavoro. Non è consentito utilizzare Internet per altri scopi e per motivi non attinenti allo svolgimento delle mansioni assegnate.
Per ragioni di sicurezza e per garantire l'integrità dei sistemi informatici, l'accesso ad Internet effettuato tramite elaboratori connessi alla rete comunale è protetto da appositi dispositivi di sicurezza informatica *(firewall, antivirus,* etc.).

Tutto il personale può connettersi alla rete Internet tramite gli strumenti a disposizione, tuttavia non è consentito:

1. registrarsi a siti, *mailing-list, forum,* bacheche elettroniche o altri servizi *online senza s*pecifica autorizzazione in tal senso da parte del responsabile di settore;
2. utilizzare applicazioni «chat-line».
3. scaricare *software,* anche se gratuito, prelevato da siti Internet, ad eccezione di quanto previsto per motivi di lavoro;
4. installare o utilizzare *software peer to peer,* finalizzato allo scambio e alla diffusione tramite la rete Internet, di materiale protetto dalla normativa vigente in tema di tutela del diritto d'autore;
5. prelevare da Internet e/o archiviare sul proprio elaboratore, ovvero sulle risorse di rete condivise, documenti informatici (testo, audio, immagini, filmati, etc.) di natura oltraggiosa, discriminatoria per sesso, religione, origine etnica appartenenza sindacale o politica o che comunque possano risultare offensivi della dignità umana.
6. diffondere attraverso Internet materiale commerciale o pubblicitario non richiesto;
7. trasmettere via Internet *virus,* worms, *trojan-horses* o altro codice maligno, noto per arrecare danni e malfunzionamenti a sistemi informatici;
8. prelevare da Internet, ovvero inviare tramite Internet, dati o altre risorse informatiche per scopi non consentiti dalle norme vigenti;
9. fornire a soggetti non autorizzati l'accesso alla connessione Internet comunale;
10. utilizzare la connessione Internet al fine di arrecare danno o disturbo a terzi;
11. effettuare transazioni commerciali e/o finanziarie di natura personale, ivi comprese operazioni di *remote banking,* acquisti *online* e simili, salvo specifica autorizzazione.

Per garantire la sicurezza della rete informatica dal rischio di accesso abusivo e dall'azione dannosa di programmi, è utilizzato un proxy server che fornisce l'elenco dei siti web visitati da tutte le postazioni esistenti senza correlarli alla singola postazione di lavoro. I sistemi informatici redigono dei report, tratti dall'analisi dei log files creati dal proxy server, indicanti i siti web visitati. Il report è accompagnato da una relazione sintetica e da una proposta dei siti da inserire in black-list per inibirne l'accesso. A seguito dell'analisi del report, della validazione della lista dei siti segnalati e dell'eventuale segnalazione di integrazioni e/o modifiche da apportare a detta lista, viene autorizzato l'inserimento in blacklist dei siti web da parte dell'Amministrazione.

Art. 7: Utilizzo della Posta Elettronica
Anche la posta elettronica (interna ed esterna) è uno strumento di lavoro. Non è consentito utilizzarla per motivi non attinenti allo svolgimento delle mansioni assegnate.
Non è comunque consentito:
1. consultare indirizzi di posta elettronica diversi da quelli assegnati dal comune;
2. inviare o memorizzare messaggi di natura oltraggiosa, discriminatoria per sesso, religione, origine etnica, appartenenza sindacale o politica o che comunque possano risultare offensivi della dignità umana.
3. la posta elettronica diretta all'esterno della rete informatica comunale può essere intercettata da estranei e, dunque, non deve essere usata per inviare documenti di lavoro strettamente riservati.

Art. 8: Responsabilità degli utenti

Gli utenti sono responsabili personalmente di tutti gli strumenti informatici loro affidati.

Per quanto non specificato nel presente documento è richiesto comunque un atteggiamento ispirato alla correttezza ed alla buona fede oltre che ai principi e ai doveri stabiliti nel Codice di comportamento dei dipendenti delle pubbliche amministrazioni

In caso di dubbi, necessità di informazioni, sospetto di tentativi di intrusione ecc., l'utente deve immediatamente comunicarlo al personale addetto ai sistemi informatici verbalmente e tramite posta interna.

Ciascun utente è responsabile per l'utilizzo da parte di terzi, anche se conosciuti o affini, degli strumenti informatici a lui affidati.

Poiché in caso di violazioni contrattuali e giuridiche, sia il comune sia il singolo lavoratore sono potenzialmente perseguibili con sanzioni, anche di natura penale, il comune verificherà, nei limiti consentiti dalla legge e dai contratti, il rispetto delle regole del presente regolamento e l'integrità del proprio sistema informatico.

La violazione da parte dei lavoratori dei principi e delle norme contenute nel presente regolamento costituisce violazione degli obblighi e dei doveri del dipendente pubblico e, pertanto, in relazione alla gravità dell'infrazione, i responsabili di settore, previo espletamento di procedimento disciplinare, possono procedere all'applicazione delle sanzioni previste dalle disposizioni contrattuali vigenti in materia.

Il presente regolamento viene consegnato a ciascun dipendente del Comune di Marcon, che firma la dichiarazione allegata.

ALLEGATO AL REGOLAMENTO PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI E DI INTERNET APPROVATO CON DELIBERAZIONE DI GIUNTA COMUNALE N. _____ DEL _____

DICHIARAZIONE DI ASSUNZIONE DI RESPONSABILITA' PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI E L'ACCESSO A INTERNET DALLE POSTAZIONI AZIENDALI

(Dichiarazione da sottoscrivere e trasmettere Settore Programmazione Controllo e Risorse Umane)

Il sottoscritto, firmando il presente documento, riconosce di aver letto, compreso e accettato integralmente le politiche e le regole del Comune di Marcon, riguardo l'utilizzo delle risorse informatiche e l'accesso a Internet.
Il sottoscritto si assume la piena responsabilità in caso di violazione delle leggi e dei regolamenti, riconducibili al suo accesso personale a internet e all'utilizzo delle strumentazioni informatiche.

nome e cognome _____

Settore _____

Marcon, _____

Firma

_____