COMUNE DI GAZZO VERONESE

.'060

c.f. 8200277 023 6

con sede a RONCANOVA

PROVINCIA DI VERONA

Allegato n. 3

Regolamento

INFORMATICO

INDICE

Premessa

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

Premesso quindi che l'utilizzo delle risorse informatiche e telematiche dell'Ente deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro, l'Ente ha adottato un Regolamento interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati.

Tali prescrizioni sono formulate in attuazione del D.Lgs. n°196/2003 sulle misure di sicurezza obbligatorie.

Art. 1
Utilizzo del Personal Computer

1. Il Personal Computer affidato al dipendente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

2. L'accesso all'elaboratore è protetto da password che deve essere custodita dall'incaricato con la massima diligenza e non divulgata. La stessa password deve essere attivata per l'accesso alla rete, per l'accesso a qualsiasi applicazione, per lo screen saver e per il collegamento a Internet. Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte dell'Amministratore di Sistema.

3. Non è consentito installare autonomamente programmi provenienti dall'esterno salvo previa autorizzazione esplicita dell'Amministratore del Sistema, perché sussiste il grave pericolo di portare Virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore.

4. Non è consentito l'uso di programmi diversi da quelli distribuiti ufficialmente dall'Ente (D.Lgs. 518/92 sulla tutela giuridica del software e L. 248/2000 nuove norme di tutela del diritto d'autore).

5. Non è consentito all'utente modificare le caratteristiche impostate sul proprio PC, salvo previa autorizzazione esplicita dell'Amministratore del Sistema.

6. Il Personal Computer deve essere spento ogni giorno prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. In ogni caso 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. Deve essere attivato lo screen saver e la relativa password.

7. Non è consentita l'installazione sul proprio PC di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem,...), se non con l'autorizzazione espressa dell'Amministratore del Sistema.

8. Agli utenti incaricati del trattamento dei dati sensibili è fatto divieto l'accesso contemporaneo con lo stesso account

9. Ogni utente deve prestare la massima attenzione ai supporti di origine esterna avvertendo immediatamente l'Amministratore del Sistema nel caso in cui siano rilevati virus ed adottando quanto previsto dal successivo punto 8 del presente Regolamento relativo alle procedure di protezione antivirus.

10. Non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

Art. 2
Utilizzo della rete dell'Ente

1. 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, nemmeno per brevi periodi, in queste unità. Su queste unità, vengono svolte regolari attività di controllo, amministrazione da parte dell'Amministratore del Sistema.

2. Le password d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite. È assolutamente proibito entrare nella rete e nei programmi con altri nomi utente.

3. L'Amministratore del Sistema può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.

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

5. È cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti. È buona regola evitare di stampare documenti o file non adatti (molto lunghi o non supportati, come ad esempio il formato pdf o file di contenuto grafico) su stampanti. In caso di necessità la stampa in corso può essere cancellata.

Art. 3
Gestione delle Password

1. Le password di ingresso alla rete, di accesso ai programmi e dello screen saver, sono previste ed attribuite dall'Amministratore del Sistema, consentita comunque l'autonoma sostituzione da parte degli incaricati al trattamento con contestuale comunicazione al gestore delle password.

2. La password, quando è prevista dal sistema di autenticazione, è composta da almeno sei caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.

3. La password deve essere immediatamente sostituita, dandone comunicazione all'Amministratore del Sistema, nel caso si sospetti che la stessa abbia perso la segretezza.

4. Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia all'Amministratore del Sistema.

5. Per la sostituzione e modifica delle passwords dovrà essere utilizzato l'allegato modulo di richiesta.

Art. 4
Utilizzo dei supporti magnetici

1. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

2. I supporti magnetici contenenti dati sensibili devono essere custoditi in archivi chiusi a chiave.

3. Non è consentito scaricare files contenuti in supporti magnetici/ottici non aventi alcuna attinenza con la propria prestazione lavorativa.

4. Tutti i files di provenienza incerta od esterna, ancorché attinenti all'attività lavorativa, devono essere sottoposti al controllo ed alla relativa autorizzazione all'utilizzo da parte dell'Amministratore del Sistema.

Art. 5
Utilizzo di PC portatili

1. L'utente è responsabile del PC portatile assegnatogli dall'Amministrato del Sistema e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel 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. Non è consentito l'utilizzo di strumentazione che non sia di proprietà dell'Ente.

3. I PC eventualmente portatili utilizzati all'esterno (convegni, visite in azienda), in caso di allontanamento, devono essere custoditi in un luogo protetto.

Art. 6
Uso della posta elettronica

1. La casella di posta, assegnata dall'Ente all'utente, è imo strumento di lavoro. Le persone assegnatarie delle caselle dì posta elettronica sono responsabili del corretto utilizzo delle stesse.

2. È fatto divieto di utilizzare le caselle di posta elettronica dell'Ente, per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mailing list salvo diversa ed esplicita autorizzazione.

3. È buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

4. Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per l'Ente, ovvero contenga documenti da considerarsi riservati in

quanto contraddistinti dalla dicitura "strettamente riservati" o da analoga dicitura, deve essere visionata od autorizzata dal Segretario Generale. In ogni modo, è opportuno fare riferimento alle procedure in essere per la corrispondenza ordinaria.

5. E possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario, ma di norma per la comunicazione ufficiale è obbligatorio avvalersi degli strumenti tradizionali (fax, posta,...).

6. Per la trasmissione di file all'interno dell'Ente, è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati.

7. È obbligatorio controllare i file attachements di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

8. È vietato inviare catene telematiche (o di Sant'Antonio). Se si dovessero ricevere messaggi di tale tipo, si deve comunicarlo immediatamente all'Amministratore del Sistema. Non si deve in alcun caso attivare gli allegati di tali messaggi.

9. L'utilizzo delle caselle di posta elettronica è regolamentata secondo gli stessi criteri e modalità previsti nei punti precedenti del presente regolamento.

Art. 7
Uso della rete Internet e dei relativi servizi

1. Il PC abilitato alla navigazione in Internet costituisce uno strumento necessario allo svolgimento della propria attività lavorativa. È assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.

2. È fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dall'Amministratore del Sistema.

3. È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dal Segretario Generale e con il rispetto delle normali procedure di acquisto.

4. È da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.

5. È 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 (o nicknames).

6. La navigazione avviene attraverso una Credenziale Personale, è registrata e risponde ai requisiti di sicurezza necessari per evitare usi impropri del servizio.

7. Tutte le registrazioni sono fatte mantenendo la privacy dell'utente e vengono distrutte periodicamente, utilizzabili solo per necessità dell'autorità giudiziaria ai sensi di legge.

8. Per quanto riguarda l'accesso ai siti Internet si adottano le seguenti procedure:

a) distribuzione di norme interne di comportamento contenute nel codice di comportamento dei dipendenti previsto dall'art. 27 del Decreto Legislativo 80/98;

b) evidenziazione a video del divieto di accesso a siti non autorizzati;

c) verifica a campione degli accessi con modalità che escludano l'identificazione di persone eventualmente contattate;

d) installazione di software-filtro che permettano di inibire o restringere l'accesso a siti non autorizzati e/o limitare i tempi di collegamento. Le modalità di individuazione e di definizione dei filtri (BLACK LIST) sono decise dal Responsabile del Sistema Informatico di concerto con il Segretario Generale.

e) L'utilizzo ampio di Internet, non soggetto cioè ai filtri di cui sopra, è concesso solo per fini strettamente istituzionali ed avviene mediante autorizzazione del Responsabile del Sistema Informatico;

9. È fatto divieto di navigare in Internet per motivi diversi da quelli legati all'attività lavorativa.

I dipendenti e i collaboratori, in particolare, sono tenuti a utilizzare Internet per le specifiche finalità della propria attività e non devono inoltre appesantire il traffico della rete con collegamenti particolarmente lunghi e complessi (es. download di file, connessioni a stazioni radio on line, applicazioni "peer to peer", chat, Skype o similari,, etc.) quando ciò non sia collegato allo svolgimento dell'attività lavorativa.

10. Per le sedi comunali ove esistono provvisoriamente connessioni internet dirette cioè non gestite dal sistema informatico comunale, la responsabilità sull'utilizzo e sull'accesso alla

rete Internet è a carico del responsabile dell'ufficio cui è stato affidato il collegamento (tipicamente di tipo ADSL). Egli può delegarne l'utilizzo a propri collaboratori/colleghi nel rispetto delle norme generali di utilizzo della rete Internet vigenti.

Art. 8
Protezione antivirus

1. Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico mediante virus o mediante ogni altro software aggressivo.

2. Ogni utente è tenuto a controllare il regolare funzionamento e l'aggiornamento periodico del software installato, secondo le procedure previste.

3. Nel caso che il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente:

a) sospendere ogni elaborazione in corso senza spegnere il computer;

b) segnalare l'accaduto all'Amministratore di Sistema.

4. Non è consentito l'utilizzo di floppy disk, e cd-rom, cd riscrivibili, nastri magnetici di provenienza ignota.

5. Ogni dispositivo magnetico di provenienza esterna all'Ente dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere consegnato all'Amministratore di Sistema.

Art. 9
Osservanza delle disposizioni in materia di Privacy

1. È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza, come indicate nella lettera di individuazione di incaricato del trattamento dei dati, ai sensi del D.Lgs. n° 196/2003.

Art. 9bis
Monitoraggio e controlli

1. Il Comune può avvalersi di sistemi di controllo sul corretto utilizzo degli strumenti di lavoro (che consentono indirettamente un controllo a distanza dell'effettivo adempimento della prestazione lavorativa e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori) esclusivamente nel rispetto di quanto previsto dal Provvedimento del Garante per la protezione dei dati personali del 1 marzo 2007 n. 13, di quanto disposto dagli artt. 2 e 15 della Costituzione, dall'art. 616, quarto comma, C.P. e dall'art. 49 del Codice dell'amministrazione digitale;

2. In particolare l'Ente, nell'effettuare controlli sull'uso degli strumenti elettronici eviterà un'interferenza ingiustificata sui diritti e sulle libertà fondamentali di lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata;

3. Le comunicazioni effettuate attraverso il servizio di posta elettronica sono riservate. Il contenuto di tali comunicazioni non può in nessun caso essere oggetto di alcuna forma di verifica, controllo o censura da parte del Comune, dell'internet provider o da parte di altri soggetti;

4. Le attività sull'uso del servizio di accesso ad Internet vengano automaticamente registrate in forma elettronica attraverso i LOG di sistema. Il trattamento dei dati contenuti nei LOG, può avvenire esclusivamente in forma anonima in modo tale da precludere l'identificazione degli utenti e/o delle loro attività;

5. I dati personali contenuti nei LOG possono essere trattati esclusivamente in via eccezionale e nelle ipotesi tassativamente di seguito indicate: per rispondere ad eventuali richieste della polizia postale e/o dell'autorità giudiziaria;

su richiesta del Responsabile del Servizio Informatico, limitatamente al caso di utilizzo anomalo degli strumenti informatici da parte degli utenti di una specifica Area/Servizio (rilevabile esclusivamente dai dati aggregati) reiterato nel tempo, nonostante un esplicito avviso circoscritto e rivolto ai dipendenti afferenti all'Area/Servizio coinvolto e un espresso invito agli stessi utenti ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite;

6. I dati contenuti nei LOG sono conservati per il tempo strettamente necessario al perseguimento di finalità organizzative, produttive e di sicurezza, comunque non superiore a 90 giorni, e sono periodicamente cancellati automaticamente dal sistema;

Art. 10
Non osservanza del regolamento dell'Ente

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

Art. 11

Aggiornamento e revisione

1. Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Le proposte verranno esaminate dall'Amministratore del Sistema e dal Segretario Generale.

2. Il presente Regolamento è soggetto a revisione con frequenza annuale.