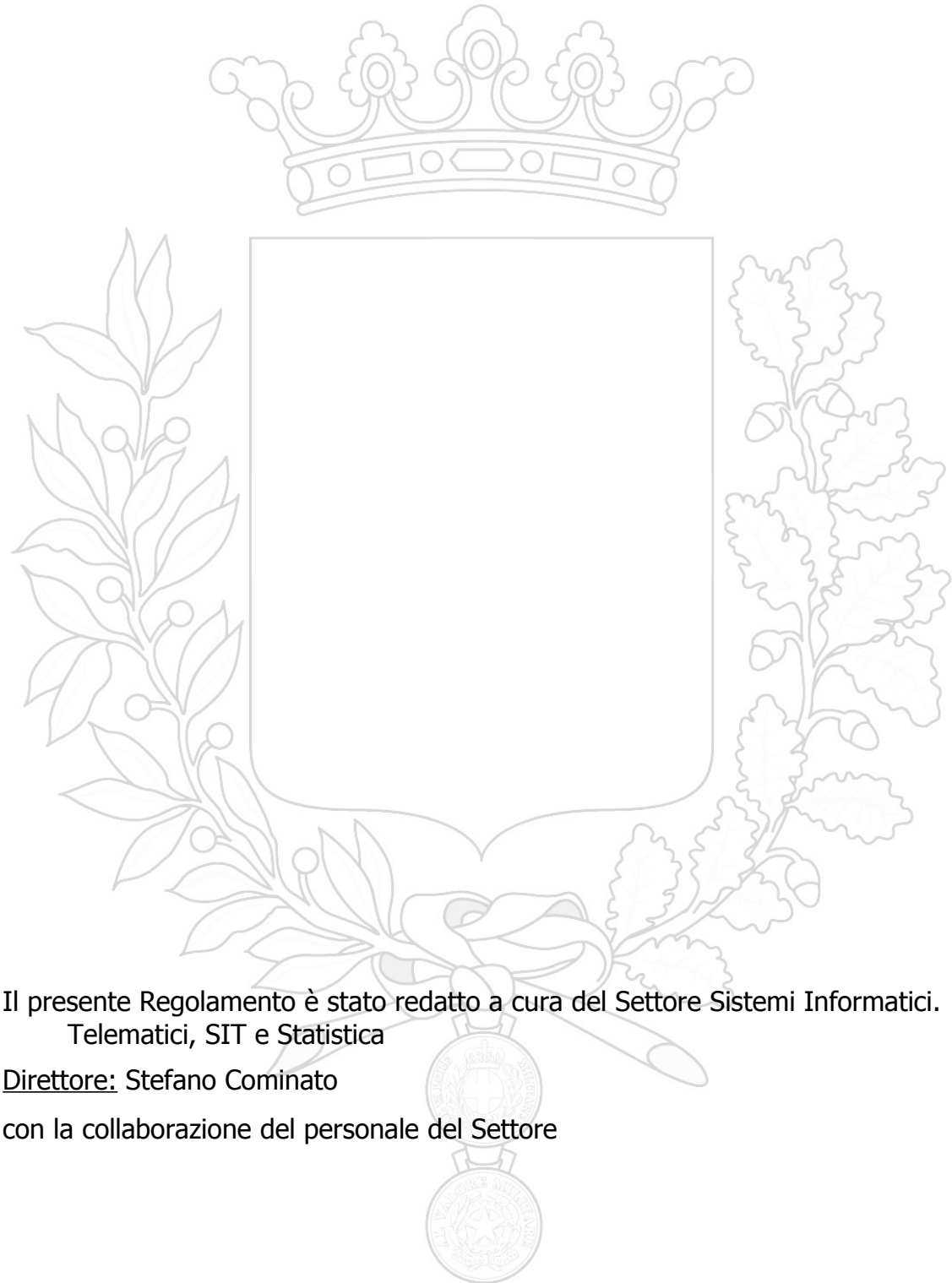
COMUNE DI VICENZA

Regolamento per l'utilizzo del Sistema Informatico Comunale

Approvato con delibera di G.C. n. 44 del 08/02/2008



Il presente Regolamento è stato redatto a cura del Settore Sistemi Informatici. Telematici, SIT e Statistica

Direttore: Stefano Cominato

con la collaborazione del personale del Settore

CAPO I

INFORMAZIONI E NORME GENERALI

a) Le informazioni formate, gestite e conservate dal Comune e i sistemi informatici a tale scopo utilizzati formano nel loro insieme il Sistema Informativo Comunale.

   Tale Sistema è un patrimonio dell'Amministrazione. E' compito di ogni collaboratore operare preservando e valorizzando questo patrimonio.

b) Il Sistema Informatico Comunale è costituito dall'insieme degli strumenti tecnologici di cui il Comune dispone per il trattamento delle informazioni, come hardware (personal computers, server di rete, stampanti e periferiche varie), software (programmi informatici di base e applicativi, database, ecc.) e reti telematiche.

c) Tutti coloro che, per qualsiasi motivo, accedono al Sistema Informatico Comunale, sono tenuti ad osservare le vigenti Leggi ed i regolamenti in materia.

d) Il Sistema Informatico Comunale può essere utilizzato dal dipendente unicamente per lo svolgimento di attività legate alla propria mansione ed ai propri incarichi.

e) Gli strumenti informatici - personal computer, stampanti, programmi, supporti magnetici, materiale di consumo, ecc. - che il Comune mette a disposizione degli utenti per lo svolgimento del proprio lavoro sono di esclusiva proprietà dell'Amministrazione e devono essere utilizzati unicamente per gli scopi dell'Amministrazione. E' quindi vietato l'utilizzo di attrezzature informatiche per scopi personali.

f) L'Amministrazione assicura l'utilizzo del Sistema Informatico Comunale unicamente a scopi leciti ed osservando le Leggi e i Regolamenti in vigore.

g) L'Amministrazione si riserva la facoltà di ricorrere contro comportamenti da parte degli utenti in contrasto con le leggi vigenti o il presente Regolamento.

CAPO II

MISURE GENERALI DI SICUREZZA

♋ Gli strumenti informatici possono essere utilizzati unicamente per gli scopi definiti dall'Amministrazione, utilizzando le procedure ed i programmi previsti.

♌ In linea generale tutte le attività e gli utilizzi dei sistemi informatici che non sono previsti e specificamente definiti non sono autorizzati.

♍ Non è consentito utilizzare strumenti informatici dell'Amministrazione per scopi personali.

♎ Le componenti del sistema informatico comunale (hardware, software, reti) sono gestite unicamente dal CED in forma diretta o tramite soggetti (imprese, consulenti, ecc.) che operano su incarico e per conto del CED. Nessun altro soggetto è autorizzato ad operare sul sistema informatico comunale.

♏ Qualsiasi richiesta di intervento tecnico di qualsiasi natura a carico del sistema informatico comunale deve essere gestita dal CED. Non è permesso intervenire autonomamente o ricorrere in modo autonomo a prestazioni tecniche fornite da soggetti esterni.

♐ Ogni utente del Sistema Informatico Comunale è tenuto ad osservare i comportamenti previsti dal presente Regolamento per garantire la massima sicurezza delle informazioni e l'integrità funzionale degli strumenti utilizzati.

♑ E' compito di ogni utente evidenziare situazioni di utilizzo non autorizzato degli strumenti informatici e di riportare al CED eventuali casi imprecisi o di difficile interpretazione.

♒ E' vietata l'installazione di programmi di qualsiasi genere o specie, se non dietro esplicita autorizzazione del Responsabile del CED.

♓ Ogni utente è tenuto a segnalare al CED qualsiasi malfunzionamento degli strumenti informatici in uso.

- Non è consentito procedere autonomamente a tentativi di correzione di errori o malfunzionamenti dei sistemi informatici, se non dietro esplicita autorizzazione e supervisione del personale del CED.
- La configurazione dei personal computer dell'Amministrazione è realizzata su un modello standard appositamente studiato per garantire la semplicità di gestione del parco macchine e la condivisione delle risorse informatiche tra tutti gli utenti del sistema informatico comunale. Di conseguenza non è permesso modificare la configurazione hardware del proprio posto di lavoro. In particolare non è permesso spostare dispositivi quali unità centrali, unità video o stampanti, scanner, telefoni o fax, e installare o disinstallare dispositivi hardware (banchi di memoria, schede, mouse, stampanti, ecc.).
- Non è permesso modificare la configurazione software dei personal computer. In particolare sono tassativamente vietate l'alterazione dei parametri di configurazione del sistema operativo, la modifica dell'interfaccia utente (attraverso l'installazione di sfondi e screen savers), e comunque qualsiasi variazione alla configurazione originale standard prevista ed implementata su tutti i personal computer dell'Amministrazione.
- Gli utenti che in seguito alla volontaria manomissione della propria postazione di lavoro provocheranno la perdita di dati o comunque malfunzionamenti a carico delle apparecchiature, saranno ritenuti responsabili degli eventuali danni subiti dall'Amministrazione.

CAPO III

L'ACCESSO AL SISTEMA INFORMATICO COMUNALE

a) L'accesso al sistema informatico comunale è consentito unicamente ai dipendenti in possesso di *credenziali di autenticazione* rilasciate dal CED. Per *credenziale di autenticazione* si intende l'insieme di **identificativo utente** e di **parola chiave** (password). Di norma l'identificativo utente è composto dal cognome dell'utente e dall'iniziale del nome uniti dal simbolo "_". Esempio: l'identificativo utente di Mario Rossi è "rossi_m).

b) Le credenziali di autenticazione sono personali e devono essere esclusivamente utilizzate dal titolare. Il titolare provvederà a custodire e a garantire la segretezza della parola chiave e a sostituirla almeno ogni tre mesi.

a) L'identificativo utente è indispensabile per poter accedere al Sistema Informatico Comunale. La UserID deve infatti essere fornita all'avvio della sessione di lavoro e permette al Sistema Informatico di riconoscere l'utente e di consentirne l'accesso alle risorse informatiche per le quali è autorizzato (cartelle su server di rete, accesso ad archivi, accesso a programmi, internet, posta elettronica, ecc.)

c) Ciascun Dirigente è responsabile della gestione delle credenziali di autenticazione dei dipendenti della propria struttura, in particolare della richiesta di nuova credenziale e di revoca di credenziale esistente. Le richieste di rilascio o di revoca di credenziali di autenticazione devono essere inoltrate in forma scritta al Dirigente del CED anche via mail. Nella richiesta il Dirigente dovrà precisare a quali risorse informatiche l'utente è abilitato ad accedere, come ad esempio archivi (database), programmi, cartelle residenti su server di rete, internet, posta elettronica, ecc.).

d) Non saranno prese in considerazioni richieste di credenziali di autenticazione formulate da soggetti diversi dal Dirigente o suo preposto.

e) In caso di cessazione dal servizio o di trasferimento ad altra struttura di un dipendente in possesso di credenziali di autenticazione, il Dirigente responsabile deve chiedere al CED la revoca delle credenziali stesse. Il Dirigente è quindi

responsabile di danni arrecati all'Amministrazione derivanti dall'accesso indebito ad archivi comunali effettuato con credenziali di dipendenti non più in servizio e non revocate (Art. 169 L.196/03 "Codice in materia di protezione dei dati personali")

CAPO III

UTILIZZO DELL'HARDWARE

a) Il CED provvede all'acquisto delle apparecchiature informatiche necessarie per l'informatizzazione degli Uffici Comunali. La tipologia, la dotazione e la configurazione delle apparecchiature informatiche e dei posti di lavoro in generale sono definiti dal CED sulla base delle esigenze degli utenti e della integrazione e compatibilità col Sistema Informatico Comunale.

b) L'installazione, configurazione e manutenzione di tutte le componenti del Sistema Informatico Comunale sono gestite dal CED.

c) E' tassativamente vietato il collegamento al Sistema Informatico Comunale di apparecchiature non di proprietà dell'Amministrazione o la connessione ad altre reti telematiche salvo specifica autorizzazione del CED.

d) Tutti i dispositivi utilizzati dagli utenti devono essere trattati con cura e deve essere segnalato qualsiasi malfunzionamento.

e) Non è autorizzato lo spostamento di alcun strumento od accessorio fuori delle sedi comunali, o tra sedi diverse, se non dopo esplicita autorizzazione da parte del Direttore di Settore competente sentito il parere del Responsabile del CED.

f) Ogni utente deve procedere allo spegnimento dei dispositivi che ha in uso alla fine dell'orario lavorativo ed in tutti i casi di assenza prolungata dal proprio posto di lavoro, con esclusione delle postazioni che per ragioni di servizio devono rimanere sempre accese (es: server di rete).

g) I dispositivi devono essere sempre spenti seguendo le procedure opportune (ad esempio spegnimento mediante chiusura della sessione di lavoro in Windows).

h) Imballi e confezioni dei dispositivi in uso devono essere conservati o consegnati al personale del CED salvo diverse disposizioni impartite dal CED stesso

i) Manuali d'uso ed altri materiali di corredo dei dispositivi in uso devono essere conservati o consegnati al personale del CED salvo diverse disposizioni impartite dal CED stesso.

j) Licenze e documentazione di acquisto devono essere consegnate al personale del CED che ne cura la conservazione ai fini amministrativi e di controllo.

k) Non si deve procedere ad operare sulle connessioni elettriche o di rete, se non dietro specifica autorizzazione. In nessun caso si deve operare sulle connessioni elettriche o di rete quando i dispositivi sono in tensione.

l) Gli utenti non sono autorizzati ad operare su dispositivi di rete, quali server, stampanti condivise, dispositivi di connessione (hub, armadi di rete, router, stampanti di rete).

CAPO IV
UTILIZZO DEI PROGRAMMI APPLICATIVI (SOFTWARE)

a) Il CED provvede all'acquisto delle licenze d'uso dei pacchetti applicativi necessari all'informatizzazione degli Uffici Comunali. Le caratteristiche del software applicativo acquistato sono definite dal CED sulla base delle esigenze degli utenti e della integrazione e compatibilità col Sistema Informatico Comunale.

b) Le licenze d'uso dei pacchetti applicativi installati nel CED sono di proprietà dell'Amministrazione.

c) I programmi applicativi sviluppati in proprio dall'Amministrazione attraverso i propri dipendenti o da terzi appositamente incaricati, al fine di soddisfare esigenze di informatizzazione delle attività degli uffici, sono di esclusiva proprietà dell'Amministrazione.

d) L'utilizzo di tutti i programmi applicativi è limitato ai casi ed agli scopi previsti dall'Amministrazione. Non è comunque consentito l'utilizzo di programmi applicativi per scopi personali.

e) Non è consentito l'accesso a programmi od a parti di programmi applicativi cui non si è autorizzati anche se non esistono misure tecniche a protezione delle stesse.

f) Non è consentita l'esecuzione di alcuna modifica ai programmi applicativi se non, in casi particolari, dopo esplicita autorizzazione del Responsabile del CED. In particolare non è consentita l'autonoma esecuzione di aggiornamenti, cambio di versioni o di lingua, spostamento di dischi o cartella di installazione.

g) A conclusione di ogni sessione di lavoro o per interruzioni di durata significativa, l'utente è tenuto a chiudere l'applicazione in uso, seguendo le procedure previste (per gli utilizzatori di sistemi in ambiente Windows, procedere alla disconnessione dell'utente).

h) E' vietata la duplicazione o copia parziale del software installato nel Sistema Informatico Comunale, con esclusione delle copie di salvataggio effettuate dal personale del CED.

i) E' vietata l'autonoma installazione di nuovi programmi applicativi, o di nuove versioni degli stessi. Ciò vale per le copie non autorizzate di software di cui l'utente fosse venuto in possesso, ma anche per copie il cui possesso è legale (acquisto, regalo, prestito) ma non fa capo all'Amministrazione.

j) L'utente deve segnalare qualsiasi malfunzionamento od errore dei programmi applicativi in uso agli addetti del Sistema Informatico nei tempi più brevi; la segnalazione deve essere chiara e completa e, se possibile, deve evidenziare le condizioni in cui si è verificato l'errore.

CAPO V

GESTIONE DEGLI ARCHIVI

a) Le informazioni prodotte dagli utenti (documenti, archivi, dati in generale) devono essere memorizzate unicamente sui dispositivi di rete (server) appositamente configurati dal CED, salvo specifiche diverse autorizzazioni scritte o per motivi legati alla conformazione della struttura della rete informatica.

b) Il CED coordina le attività volte a garantire la sicurezza delle informazioni memorizzate sui server di rete attraverso periodiche copie di salvataggio degli archivi. Tale attività viene svolta direttamente dal personale del CED per i server collegati telematicamente con la sala macchine del CED attraverso reti a larga banda. Per gli altri casi il CED si avvale della collaborazione di "referenti" di Settore appositamente incaricati che coadiuvano i tecnici del CED nella gestione dei supporti di memorizzazione (cassette) e nella verifica della corretta esecuzione delle copie.

c) Sui server di rete viene definita per ciascun Settore/Ufficio una specifica cartella; ciascun utente potrà accedere solamente ai dati contenuti all'interno della cartella (e sottocartelle) del Settore di appartenenza, salvo eccezioni dettate da esigenze organizzative.

d) Gli archivi che contengono i dati generati dai singoli utenti sono divisi in specifiche sottocartelle nominative. Queste sottocartelle di tipo PUBBLICO non hanno alcun tipo di restrizione di accesso in lettura e quindi ogni utente può accedere alle informazioni memorizzate da qualsiasi altro utente del proprio Settore/Ufficio fatta salva la limitazione alla modifica ed alla cancellazione. Scopo di queste cartelle è la "condivisione" delle informazioni tra gli utenti dello stesso Settore/Ufficio.

e) Per esigenze organizzative sono anche generate cartelle di tipo PRIVATO per limitare l'accesso, in modifica o in lettura, ad un solo utente o gruppo un gruppo di utenti; scopo di queste cartelle è la gestione di documenti riservati.

f) I singoli utenti sono responsabili della integrità e riservatezza delle informazioni memorizzate sui server di rete nelle cartelle alle quali hanno accesso.

g) Le informazioni eventualmente memorizzate sui dischi locali dei computer non sono protette e non vengono copiate durante l'esecuzione delle copie di salvataggio effettuate dal CED. Gli utenti saranno responsabili della perdita dei dati eventualmente memorizzati su dispositivi locali rispondendo degli eventuali danni subiti dall'Amministrazione.

h) Gli utenti non sono autorizzati alla cancellazione di files o gruppi di files dei quali non conoscono scopo e/o contenuto. Gli utenti hanno la facoltà unicamente di cancellare dai dispositivi in loro uso i files che hanno personalmente creato rispondendo degli eventuali danni subiti dall'Amministrazione.

i) Nel caso sia necessaria l'eliminazione di files per mancanza di spazio sui dischi di rete, tale operazione dovrà essere svolta con la supervisione degli addetti del CED.

j) Non è consentita la copia di archivi contenenti dati dell'Amministrazione di qualsiasi genere o specie su dispositivi asportabili (floppy disk, CD/DVD, USB pen drive, nastri e simili) né su dispositivi di memorizzazione esterni all'azienda (ad esempio in server accessibili mediante Internet) se non per attività istituzionali e dietro esplicita autorizzazione dell'Amministrazione.

k) E' vietata la copia di archivi contenenti dati personali su dispositivi asportabili (floppy disk, CD/DVD, USB pen drive nastri e simili) o su dispositivi di memorizzazione esterni all'azienda (ad esempio in server accessibili mediante Internet) se non per attività istituzionali consentite da norme di legge o di regolamento e dietro esplicita autorizzazione del Responsabile del Trattamento dei dati.

l) Il CED, nell'ambito delle proprie attività di gestione e manutenzione del parco macchine, effettua controlli periodici sui personal computer in uso agli utenti e in particolare sui dispositivi di memorizzazione locale. Gli archivi, i programmi installati e le modifiche alla configurazione del PC non precedentemente autorizzati saranno cancellati ed il comportamento non autorizzato verrà segnalato al Dirigente Responsabile di competenza ed al Settore Personale.

CAPO VI

RISERVATEZZA DELLE INFORMAZIONI

♋♑ Il sistema informatico comunale gestisce dati personali così come definiti dalla Legge 196/03 sulla tutela dei dati personali. Ogni comportamento da parte degli utilizzatori del Sistema informatico deve essere quindi conforme a quanto previsto dalla Legge e dai regolamenti.

♌♑ Ogni utente ha accesso unicamente ai dati per i quali è stato autorizzato al trattamento. Questo si riferisce in generale a tutte le informazioni trattate dal Sistema Informativo Comunale, ed in particolare ai dati personali, per i quali l'Amministrazione assicura l'osservanza delle normative di legge.

b) Tutte le informazioni dell'Amministrazione sono riservate all'utilizzo ed alla circolazione unicamente all'interno del Comune, tranne nei casi diversi esplicitamente previsti.

c) Nessuna informazione deve essere trattata, comunicata e diffusa all'esterno del Comune se non nei casi previsti dalla Legge o dai Regolamenti.

d) Ogni ciascun utilizzatore del Sistema Informatico Comunale possiede una propria e personale credenziale di autenticazione composta da un Identificativo Utente (UserID) e una Parola Chiave (Password) rilasciata dal CED su richiesta del Dirigente responsabile. L'utente è responsabile della loro custodia e non è autorizzato per Legge a comunicarla a terzi.

e) L'utente può autonomamente modificare in qualsiasi momento la propria parola chiave. Egli è comunque obbligato dalle leggi vigenti a cambiarla almeno una volta ogni tre mesi e in caso di violazione della sua segretezza.

f) L'utente che desidera modificare la parola chiave in uso deve seguire le procedure indicate dal CED.

g) I documenti riservati devono essere di norma custoditi su cartelle riservate dei server di rete.

h) E' vietata la cifratura di documenti effettuata autonomamente dal dipendente se non in casi particolari e con l'autorizzazione del Dirigente responsabile al quale deve comunque essere consegnata copia della chiave di cifratura.

i) Ai sensi dell'Art.10 del Disciplinare tecnico allegato alla L.196/03, il Titolare e il Responsabile del Trattamento dati possono richiedere agli Amministratori del CED la disponibilità di dati o strumenti elettronici assegnati ad un dipendente in caso di sua prolungata assenza o di impedimento. Ciò avviene attraverso la sostituzione della password del dipendente effettuata dall'Amministratore dei Sistemi Informatici che la comunica al Titolare/Responsabile. L'Amministratore che ha provveduto alla sostituzione della password comunica tempestivamente e per iscritto al dipendente l'avvenuto cambio delle credenziali di accesso e le motivazioni.

j) Non è di norma permesso l'utilizzo di screen savers con blocco del PC tramite password. In caso di necessità il dipendente lo può attivare previa comunicazione al CED e al proprio Dirigente della password di sblocco.

k) L'utilizzo improprio della parola chiave, ad esempio per occultare documenti od errori commessi è considerato illecito dall'Amministrazione, che è eventualmente autorizzata a procedere nei confronti dell'utente ai sensi del C.C.N.L. e delle leggi vigenti.

CAPO VII
UTILIZZO DI INTERNET

a) L'Amministrazione Comunale mette a disposizione dei propri dipendenti l'utilizzo della navigazione Internet sulla base delle esigenze di ufficio e delle disposizioni emanate in materia dagli Organi competenti.

b) L'abilitazione per il dipendente all'utilizzo della navigazione Internet deve essere richiesta per iscritto al CED dal Dirigente responsabile anche via mail.

c) Non è consentito l'utilizzo dell'accesso ad internet per motivi personali.

d) L'Amministrazione non è responsabile di eventuali dati personali, anche di tipo sensibile, che potrebbero risultare automaticamente memorizzati all'interno di postazioni di lavoro assegnate ad utenti che, contravvenendo alla precedente disposizione, abbiano consultato per uso personale siti a carattere politico, sindacale o religioso.

e) Non è consentito comunicare informazioni personali - anche se non riguardano l'Amministrazione - nei siti visitati durante la navigazione, eccetto che per motivi strettamente legati alla propria attività e dopo esplicita autorizzazione del proprio Dirigente.

f) E' tassativamente vietato il **download** (memorizzazione sul disco del proprio computer o su altri dispositivi di memorizzazione, anche rimovibili) di files od archivi di qualsiasi genere trovati durante la navigazione su Internet, se non per motivi strettamente legati alla propria attività. In particolare è vietato il download di contenuti protetti dalle leggi sul diritto d'autore (software, brani musicali, films, fotografie, ecc.)

g) Nel caso di scarico autorizzato di files da Internet, il file deve essere immediatamente verificato con il software antivirus.

h) Non è ammessa la comunicazione di dati dell'Amministrazione in siti o sistemi di posta elettronica, se non dietro autorizzazione e per motivi direttamente collegati alla propria attività.

i) L'Amministrazione adotta sistemi automatici di filtraggio degli indirizzi Internet (URL filtering) per impedire l'accesso da parte degli utenti a siti non di carattere istituzionale. Gli stessi sistemi regolamentano l'accesso ad Internet in base all'orario ed al giorno della settimana impedendo, di norma, l'accesso alla rete al di fuori dell'orario di servizio. Le modalità di filtraggio degli indirizzi internet è diversificata (da filtraggio basso a filtraggio elevato) in base alle esigenze ed alle attività dei Settori. Tali esigenze sono segnalate per iscritto dai Dirigenti interessati al Responsabile CED anche via mail.

j) L'Amministrazione può avvalersi dei medesimi sistemi di cui al punto precedente anche ai fini di documentare il traffico internet generato dalla stazioni di lavoro. Tali informazioni sono raccolte unicamente allo scopo di verificare *ex-post* utilizzi illeciti del collegamento ad Internet che abbiano causato danni all'Amministrazione, o per controlli difensivi, oppure nell'ambito di indagini condotte dall'Autorità Giudiziaria. La raccolta e la custodia sono effettuate nelle modalità previste dalla normativa vigente e la garanzia e tutela delle informazioni trattate saranno assicurate in osservanza delle disposizioni di Legge in materia di Privacy e degli atti emanati dal Garante.

k) Le informazioni di cui al punto precedente sono custodite per la durata massima indicata dalle leggi vigenti e poi sono distrutte. L'accesso ai dati è consentito unicamente al Responsabile del trattamento dati e si effettuerà unicamente nei modi previsti dall'Art. 11 del D.Lgs. 196/03 ed in particolare secondo principi di gradualità dei controlli, pertinenza e non eccedenza.

l) I sistemi informatici di cui sopra non sono in alcun modo abilitati al "controllo a distanza del lavoratore" e quindi non sono in contrasto con le norme contenute nello "Statuto dei Lavoratori"

CAPO VIII

UTILIZZO DELLA POSTA ELETTRONICA

a) L'Amministrazione Comunale mette a disposizione dei propri dipendenti l'utilizzo di un sistema informatico di posta elettronica sulla base delle esigenze di ufficio e delle disposizioni emanate in materia dagli Organi competenti (Dipartimento Funzione Pubblica, Dipartimento per l'Innovazione e le Tecnologie, CNIPA, ecc.)

b) Non è permesso l'utilizzo delle caselle di posta fornite dall'Amministrazionei per motivi personali.

c) Le caselle di posta elettronica sono di esclusiva proprietà dell'Amministrazione. Non è prevista la creazione di caselle e-mail per uso personale del dipendente.

d) Le caselle possono essere intestate a Settori, uffici o singole unità operative. A queste potranno accedervi singoli dipendenti o gruppi di dipendenti a seconda delle esigenze organizzative. In caso di accesso consentito a gruppi di utenti saranno generate singole credenziali per ciascun componente del gruppo. Tali credenziali dovranno essere custodite nei modi disciplinati dal presente Regolamento.

e) Le caselle possono essere intestate in taluni casi a singoli utenti. L'assegnazione di una casella di posta elettronica con un indirizzo riportante il nome del dipendente non sottintende un uso personale della stessa come evidenziato dal nome del dominio (comune.vicenza.it) e quindi la "personalità" dell'indirizzo non implica "privatezza" dello stesso.

f) I titolari di una casella di posta elettronica con un indirizzo riportante il proprio nominativo (es: gbianchi@comune.vicenza.it) sono tenuti ad indicare in calce alle proprie e-mail un avvertimento ai destinatari nel quale sia dichiarata la natura non personale dei messaggi stessi, precisando che le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente.

g) La creazione di un nuovo indirizzo di posta elettronica deve essere richiesto dal Dirigente responsabile per iscritto al CED anche via mail, specificando il nominativo del dipendente cui è assegnato (referente).

h) Le caselle di posta elettronica devono essere di norma consultate ogni giorno. In caso di assenza prolungata del referente, il Dirigente Responsabile dovrà provvedere ad assegnare la delega alla consultazione della casella ad altro dipendente.

i) I referenti devono provvedere a eliminare periodicamente i messaggi più vecchi, ovvero a salvare su server di rete gli allegati per evitare la saturazione dello spazio della casella.

j) L'invio di messaggi che configurano impegni per il Comune (come ad esempio ordini a fornitori, ecc.) deve sempre seguire la procedura di approvazione prevista ed in particolare l'apposizione della segnatura di protocollo; non è permesso utilizzare il sistema di posta elettronica per modificare le procedure esistenti, neanche nei casi di particolare urgenza.

k) Per motivi di sicurezza informatica è vietato l'utilizzo di caselle personali di posta elettronica esistenti presso domini esterni ed accessibili via browser utilizzando i sistemi dell'Amministrazione.

l) Non è ammessa la comunicazione di dati aziendali in siti o sistemi di posta elettronica, se non dietro autorizzazione e per motivi direttamente collegati alla propria attività.

CAPO VIII
PROTEZIONE ANTIVIRUS

a) Ogni utente è tenuto a tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico Comunale da parte di virus o di ogni altro software che operi con lo scopo di superare le difese di sicurezza del sistema stesso.

b) Ogni utente è tenuto a controllare il regolare funzionamento ed aggiornamento del software antivirus installato, secondo le procedure definite dal Servizio Informatica.

c) Nel caso in cui il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente:
   - sospendere ogni elaborazione in corso senza spegnere il computer;
   - segnalare l'acceduto all'Amministratore del sistema.

d) Non è consentito l'utilizzo di dispositivi asportabili (floppy disk, CD/DVD, USB pen drive, nastri e simili) personali o comunque non proveniente dall'Amministrazione. Si consiglia di evitare la navigazione Internet su siti non istituzionali o la cui affidabilità non è accertabile. Si consiglia inoltre di non aprire files allegati ad e-mail provenienti da utenti sconosciuti.

e) Ogni dispositivo magnetico di provenienza esterna all'azienda dovrà essere verificato mediante il programma antivirus prima del suo utilizzo, e, nel caso in cui venissero rilevati virus, dovrà essere consegnato al Responsabile dei Sistemi Informatici.

CAPO IX

ACCESSO AD ARCHIVI CONTENENTI DATI PERSONALI (D.LGS. 196/03 "CODICE SULLA PRIVACY")

α) Il Comune di Vicenza, per perseguire le proprie finalità istituzionali, gestisce archivi contenenti dati personali tutelati dalla normativa in materia di *Privacy*. A tal proposito la Giunta Comunale ha nominato *Responsabili del Trattamento dei dati* i Direttori di Settore ognuno per gli archivi di propria competenza.

β) L'accesso agli archivi contenenti dati personali (comuni e/o sensibili) è consentito esclusivamente agli utenti autorizzati, detti anche *Incaricati del Trattamento dati.* L'accesso viene consentito attraverso specifiche abilitazioni dell'Identificativo e della password dell'utente.

χ) Gli Incaricati del trattamento dei dati sono individuati e nominati direttamente dal Responsabile del trattamento sulla base dell'analisi delle esigenze di servizio del Settore.

δ) All'atto della nomina, gli Incaricati del trattamento riceveranno precise indicazioni sul tipo di trattamento dei dati che sarà loro consentito (lettura, modifica, cancellazione, stampa, esportazione, importazione).

ε) Nella gestione di archivi tutelati dalla normativa sulla Privacy gli Incaricati dovranno attenersi a quanto previsto dal proprio Responsabile del trattamento. In particolare l'accesso ad archivi contenenti dati personali deve essere tassativamente circoscritto alle sole informazioni strettamente necessarie per adempiere ai compiti loro assegnati.

l) L'incaricato del trattamento di dati personali non può allontanarsi dal proprio posto di lavoro anche per brevi periodi senza aver prima chiuso la propria sessione di lavoro ("logoff" o "chiudi sessione").

CAPO IX

TUTELA DEL PATRIMONIO DELL'ENTE E RISPETTO DELLA RISERVATEZZA E DELLA DIGNITA' DEL LAVORATORE

♋ La politiche dell'Amministrazione in materia di tutela del patrimonio dell'Ente e di rispetto della riservatezza e della dignità del lavoratore si ispirano alle linee guida del *Gruppo di lavoro dei Garanti Europei* ed applicano la normativa italiana e comunitaria.

♌ L'Amministrazione, nella gestione del sistema informatico comunale, opera ricercando un bilanciamento tra il diritto alla riservatezza dei lavoratori e gli interessi legittimi dell'Ente e tra questi ultimi il diritto di tutelarsi contro le responsabilità e i danni cui possono dare origine gli atti dei lavoratori. Tale bilanciamento è attuato in base a principi di proporzionalità e di trasparenza delle azioni e delle misure adottate nei confronti dei lavoratori. Altro principio guida è quello della prevenzione di atti o comportamenti illeciti o cioè riguarda quelle azioni messe in atto dall'Ente orientate a prevenire comportamenti illeciti che possono avere conseguenze dannose evitando così il ricorso a restrizioni drastiche nell'uso degli strumenti informatici o alla sorveglianza individuale e continuativa.

♍ I sistemi informatici comunali ed in particolare quelli preposti al trattamento dei dati personali o delle informazioni pubblicate su Internet (server web), raccolgono informazioni tecniche (log monitoraggio) riguardanti l'utilizzo delle apparecchiature. Tali informazioni sono utilizzate per la tutela del sistema informatico comunale al fine di identificare accessi e utilizzi illeciti ai sistemi ed alle informazioni e consentire l'adozione di adeguate misure di sicurezza informatica. L'implementazione di questi sistemi di monitoraggio è attuata in osservanza all'Art.33 del D.Lgs. 196/03 ed alle specifiche tecniche internazionali in materia di sicurezza informatica (ISO 27000).

♎ I controlli effettuati dall'Amministrazione utilizzando le informazioni di cui al punto precedente saranno attuati solamente *ex-post* per soddisfare innanzitutto esigenze statistiche di controllo di sicurezza del funzionamento del sistema informatico e ai fini del controllo della spesa per servizi telematici. Potranno essere

inoltre utilizzati per la individuazione di accessi non autorizzati a sistemi ed informazioni o di comportamenti illeciti evidenziati dalla presenza nei sistemi informatici di virus, programmi software o altro materiale protetto da diritti d'autore (brani musicali, films, ecc.) privi di licenza d'uso. Tali verifiche, così come stabilito dalla giurisprudenza in materia (Corte dei Conti 13/11/2003), sono effettuate "ex-post" ai fini del cosiddetto *controllo difensivo* escludendo qualsiasi forma di controllo continuativo a distanza del lavoratore.

Le fattispecie oggetto di controllo difensivo sono quelle disciplinate dal Codice Penale in materia di rati informatici ed in particolare: Art. 420 C.P. "Attentato ad impianti di pubblica utilità", Art. 615 ter "Accesso abusivo ad un sistema informatico", Art. 615 quinquies "Diffusione di programmi diretti ad interrompere o a danneggiare un sistema informatico", Art. 635 bis "Danneggiamento di sistemi informatici e telematici"

- L'esercizio dei controlli difensivi sono attuati secondo i citati principi di gradualità e proporzionalità e prendono il via da controlli di tipo statistico su informazioni di tipo anonimo (es: numero e durata delle connessioni per settore, per ufficio, ecc.) e solo in caso di accertata violazione di legge o di danno per l'Amministrazione possono riguardare altre informazioni che sono sempre trattate secondo i principi di pertinenza e non eccedenza.
- La custodia delle informazioni tecniche (log monitoraggio) riguardanti l'utilizzo dei sistemi è assicurato dal Responsabile del Trattamento dati e cioè dal Responsabile CED che previene qualsiasi accesso illecito a tali dati. A tal proposito sono adottate adeguate misure di sicurezza informatica.