CITTÀ DI TROINA

Medaglia d'oro al Merito Civile

Regolamento per l'utilizzo del Sistema Informatico Comunale e dei Servizi di Telefonia e modalità di controllo del Comune di Troina

Approvato con delibera di G.C. n. ____ del _____

Il presente Regolamento è stato redatto a cura dei Servizi Informatici e Tecnologici.

Responsabile: Geom. Alessandro Nasca

Collaboratore Amministrativo: Rag. Maria Antonia Giambello

INDICE

Premessa

Negli ultimi anni l'organizzazione del lavoro è stata sottoposta ad un imponente processo di informatizzazione e, in tale contesto, i servizi di rete, tra cui posta elettronica e Internet, sono diventati strumenti quotidiani indispensabili per l'esercizio dell'attività lavorativa.

Tuttavia l'uso di tali strumenti in maniera non corretta, anche a seguito di comportamenti inconsapevoli, può essere causa di gravi minacce e problemi per la sicurezza del sistema e delle informazioni in esso contenute.

A ciò aggiungasi che le informazioni trattate nell'ambito dell'attività lavorativa possono riguardare la sfera personale dei lavoratori e di terzi per cui le attività di monitoraggio cui possono essere sottoposte le risorse informatiche, messe a disposizione sia al personale dell'Ente che alle ditte, consulenti, ecc… esterni incaricati dall'Ente, dovranno sempre ispirarsi al rispetto della normativa sulla tutela della riservatezza dei dati personali nonché ai principi di diligenza e correttezza.

Finalità

Il presente regolamento, quindi, persegue le seguenti finalità:

- adottare indirizzi trasparenti, capaci di comunicare con estrema chiarezza ai lavoratori le corrette modalità di utilizzo degli strumenti informatici assegnatigli per lo svolgimento delle mansioni loro attribuite;
- definire con altrettanta chiarezza il diritto dell'Ente a verificare l'uso corretto dei suddetti strumenti nonchè le modalità con le quali lo stesso esercita tale diritto di verifica.

Per quanto non espressamente previsto dal presente atto, si rinvia alle disposizioni generali vigenti in materia, con particolare riferimento alle Linee Guida del Garante per Posta Elettronica e Internet (Delib. Garante Privacy n. 13 del 1° marzo 2007), ed alla Direttiva della Presidenza del Consiglio dei Ministri - Dipartimento della Funzione Pubblica- n. 2/2009.

L'Amministrazione comunale è tenuta ad assicurare la funzionalità degli strumenti informatici assegnati ai lavoratori e si impegna a promuovere ogni opportuna misura, organizzativa e tecnologica, volta a prevenire il rischio di utilizzi impropri delle strumentazioni e delle banche dati di proprietà dell'Ente.

Ambito di applicazione

La rete del Comune di Troina è costituita dall'insieme delle risorse informatiche, cioè dalle risorse infrastrutturali e dal patrimonio informativo digitale, nonché, i servizi di telefonia.

Le risorse infrastrutturali sono le componenti hardware/software e gli apparati elettronici collegati alla rete informatica comunale. Il patrimonio informativo è l'insieme delle banche dati in formato digitale ed in generale tutti i documenti prodotti tramite l'utilizzo dei suddetti apparati.

I servizi di telefonia sono costituiti dall'insieme delle infrastrutture telefoniche in dotazione, in particolare dalle linee e dagli apparecchi telefonici.

Il presente Regolamento si applica a tutti gli utenti che a diverso titolo sono autorizzati ad accedere alla rete comunale. Per utenti si intendono gli amministratori, i responsabili di settore, i dipendenti a tempo indeterminato e determinato, ed i collaboratori impiegati a diverso titolo presso l'Ente, compreso il personale fornito da terze parti.

I fornitori esterni, addetti alla manutenzione di hardware, software e reti, operano in conformità alle presenti disposizioni, sotto la sorveglianza dell’Amministratore di Sistema.

Principi generali

Gli strumenti informatici forniti al personale devono essere utilizzati esclusivamente per lo svolgimento del lavoro assegnato con modalità e comportamenti adeguati ai compiti ed alle responsabilità dei dipendenti pubblici, nel rispetto delle comuni regole previste per la sicurezza dei sistemi informatici e per la tutela dei dati.

Ciascun dipendente è responsabile, per l'utilizzo anche da parte di terzi, degli strumenti informatici a lui affidati. Per strumenti informatici si intendono: personal computer fissi o portatili, videoterminali, stampanti locali e/o di rete, i prodotti software regolarmente licenziati, palmari, cellulari o altri dispositivi di telecomunicazione, le relative periferiche nonché tutta l’infrastruttura logica e fisica che permette l’interconnessione delle postazioni di lavoro al fine di agevolare la trasmissione di dati.

Il dipendente deve custodire la propria strumentazione in modo appropriato e diligente, segnalando tempestivamente ogni danneggiamento, furto o smarrimento al proprio Responsabile di Servizio e all’Amministratore di Sistema.

E' tassativamente proibito installare programmi provenienti dall’esterno, in quanto l'utilizzo di software non regolarmente acquistato dall’Ente può configurare un reato ed essere causa di diffusione di virus informatici, oltre a costituire un grave pericolo per la stabilità delle applicazioni dell’elaboratore.

Le aree di memorizzazione condivise in rete, sono spazi di condivisione di informazioni messe a disposizione dall’Ente per lo svolgimento dell’attività lavorativa e non possono in alcun modo essere utilizzate per scopi diversi. Su queste unità vengono svolte regolari attività di verifica e/o back-up da parte degli addetti ai Servizi Informatici e Tecnologici, i quali potranno, in qualunque momento, procedere alla rimozione di ogni file e/o applicazione che riterranno pericolosi per la sicurezza e/o non inerenti all’attività lavorativa sia sui PC dei dipendenti sia sulle unità di rete. La stessa facoltà, sempre ai fini di garantire la salvaguardia e la sicurezza del sistema informatico e per ulteriori motivi tecnici e manutentivi, si applica anche in caso di assenza prolungata o impedimento dell’utente.

Costituisce buona regola la periodica pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione, inoltre, deve essere prestata alla duplicazione dei dati. È, infatti, assolutamente da evitare un’archiviazione ridondante che non consenta in modo chiaro ed inequivocabile, l’identificazione dello stato di revisione di un documento.

L’utilizzo degli strumenti informatici al di fuori dell’orario di servizio è consentito solo previa autorizzazione del proprio Responsabile di Servizio. Infine, il dipendente è tenuto ad osservare le direttive dell’Amministratore di Sistema volte a garantire il corretto funzionamento delle procedure di backup le quali possono essere reperite al link che sarà comunicato dagli stessi.

Contesto normativo

I principi applicati nella stesura del Regolamento sono tratti dal quadro normativo che segue:

- Art. 15 Costituzione;
- Norme del codice civile: artt. 2087, 2104, 2105 e 2106;
- L. 20 maggio 1970, n. 300 (Statuto dei lavoratori) - artt. 4 e 8;
- Allegato VII, par. 3, D. Lgs. 19 settembre 1994, n. 626 e succ. mod. in materia di sicurezza sul lavoro;
- Codice in materia di protezione dei dati personali (D. Lgs. n. 196/2003);
- Art. 49, D.Lgs. 7 marzo 2005 n. 82, Codice dell'amministrazione digitale, "Segretezza della corrispondenza trasmessa per via telematica" e s.m.i.;
- "Linee guida del Garante per posta elettronica e Internet", emanate con deliberazione 1 marzo 2007 n. 13.

ART. 1
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 (da ora denominato SIC). Tale Sistema è un patrimonio dell'Ente. È compito di ogni collaboratore operare preservando e valorizzando questo patrimonio.
b) Il SIC è costituito dall'insieme degli strumenti tecnologici di cui il Comune dispone per il trattamento delle informazioni, come hardware (personal computer da ora denominato PC, server di rete, stampanti, fotocopiatrici 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, fotocopiatrici, 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 dello stesso e devono essere utilizzati unicamente per gli scopi dell'Ente. È quindi vietato l'utilizzo di attrezzature informatiche per scopi personali.
f) L'Ente assicura l'utilizzo del Sistema Informatico Comunale unicamente a scopi leciti ed osservando le Leggi e i Regolamenti in vigore.
g) L'Ente si riserva la facoltà di ricorrere contro comportamenti da parte degli utenti in contrasto con le leggi vigenti e/o il presente Regolamento.

ART. 2
MISURE GENERALI DI SICUREZZA

a) Gli strumenti informatici possono essere utilizzati unicamente per gli scopi definiti dall'Ente, utilizzando le procedure ed i programmi previsti.
b) In linea generale tutte le attività e gli utilizzi dei sistemi informatici che non sono previsti e specificamente definiti non sono autorizzati.
c) Non è consentito utilizzare strumenti informatici dell'Ente per scopi personali.
d) Le componenti del SIC (hardware, software, reti) sono gestite unicamente dal personale dei Servizi Informatici e Tecnologici in forma diretta o tramite soggetti (imprese, consulenti, ecc.)

che operano su incarico e per conto degli stessi. Nessun altro soggetto è autorizzato ad operare sul SIC.

e) Qualsiasi richiesta di intervento tecnico di qualsiasi natura a carico del SIC deve essere gestita e autorizzata dall'Amministratore di Sistema. Non è permesso intervenire autonomamente o ricorrere in modo autonomo a prestazioni tecniche fornite da soggetti esterni anche se in convenzione con l'Ente.

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

g) E' compito di ogni utente evidenziare situazioni di utilizzo non autorizzato degli strumenti informatici e di segnalare all'Amministratore di Sistema, eventuali casi imprecisi o di difficile interpretazione.

h) È vietata l'installazione di programmi di qualsiasi genere o specie, se non dietro esplicita autorizzazione dell'Amministratore di Sistema.

i) Ogni utente è tenuto a segnalare agli Amministratori di Sistema qualsiasi malfunzionamento degli strumenti informatici in uso.

j) La configurazione dei PC dell'Ente è realizzata su modelli valutati dall'Amministratore di Sistema, al fine di 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 PC. In particolare non è permesso spostare dispositivi quali unità centrali, unità video o stampanti, fotocopiatrici, scanner, telefoni o fax, e installare o disinstallare dispositivi hardware (banchi di memoria, schede, mouse, stampanti, ecc.) se non a seguito di autorizzazione dell'Amministratore di Sistema.

k) Non è permesso modificare la configurazione software dei PC. In particolare sono tassativamente vietate l'alterazione dei parametri di configurazione del sistema operativo.

l) 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 arrecati all'Ente.

ART. 3
L'ACCESSO AL SISTEMA INFORMATICO COMUNALE

a) L'accesso al SIC è consentito unicamente ai dipendenti in possesso di credenziali di autenticazione rilasciate dall'Amministratore di Sistema. Per credenziale di autenticazione si intende l'insieme di identificativo utente e di parola chiave (password). Di norma

l'identificativo utente è composto dall'iniziale del nome e dal cognome dell'utente. Esempio: l'identificativo utente di Mario Rossi è "mrossi".

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.

c) L'identificativo utente è indispensabile per poter accedere al SIC. 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.).

d) L'Amministratore di Sistema è responsabile della gestione delle credenziali di autenticazione dei dipendenti. Ai Responsabili di Settore compete la 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 all'Amministratore di Sistema anche via mail. Nella richiesta il Responsabile di Settore 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.

e) Non saranno prese in considerazioni richieste di credenziali di autenticazione formulate da soggetti diversi dal Responsabile di Settore.

f) In caso di cessazione dal servizio o di trasferimento ad altro settore di un dipendente in possesso di credenziali di autenticazione, il Responsabile del Settore di provenienza, deve chiedere all'Amministrazione di Sistema la revoca delle credenziali stesse. Il Responsabile di Settore è quindi responsabile di danni arrecati all'Ente 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").

ART. 4
UTILIZZO DELL'HARDWARE

a) I Servizi Informatici e Tecnologici provvedono all'acquisto delle apparecchiature informatiche necessarie per l'informatizzazione degli Uffici Comunali. La tipologia, la dotazione e la configurazione delle apparecchiature informatiche e postazioni di lavoro, in generale, sono definiti dallo stesso Servizio sulla base delle esigenze degli utenti e della integrazione e compatibilità col SIC.

b) L'installazione, configurazione e manutenzione di tutte le componenti del SIC sono gestite dal personale dei Servizi Informatici e Tecnologici in proprio o attraverso l'ausilio di personale esterno all'uopo incaricato.
c) È tassativamente vietato il collegamento al SIC di apparecchiature non di proprietà dell'Ente o la connessione ad altre reti telematiche salvo specifica autorizzazione dell'Amministratore di Sistema
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 Responsabile di Settore competente sentito il parere dell'Amministratore di Sistema.
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) Manuali d'uso ed altri materiali di corredo dei dispositivi in uso devono essere conservati o consegnati al personale dei Servizi Informatici e Tecnologici salvo diverse disposizioni impartite dallo stesso Servizio.
i) Licenze e documentazione di acquisto devono essere consegnate al personale dei Servizi Informatici e Tecnologici che ne cura la conservazione ai fini amministrativi e di controllo.
j) 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.
k) Gli utenti non sono autorizzati ad operare su dispositivi di rete, quali server, stampanti condivise, fotocopiatrici, dispositivi di connessione (hub, armadi di rete, router, stampanti di rete).

ART. 5
UTILIZZO DI PERSONAL COMPUTER PORTATILI

a) I Responsabili di Settore, qualora ritengano necessaria l'assegnazione di PC portatili ad uso del proprio personale, dovranno inoltrare apposita richiesta motivata al Responsabile dei Servizi Informatici e Tecnologici. In linea di massima, l'assegnazione del PC portatile prevede la

restituzione di quello fisso e l'installazione di tastiera, mouse e monitor per facilitarne l'utilizzo nella propria postazione.

b) Il Responsabile di Settore vigila sul corretto utilizzo del PC portatile e ne è corresponsabile assieme al lavoratore che deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

c) L'utilizzo del PC portatile è soggetto alle stesse regole previste per i PC fissi connessi in rete; non è pertanto cedibile a terzi estranei all'Ente e deve essere utilizzato ai soli fini istituzionali.

ART. 6
UTILIZZO DEI PROGRAMMI APPLICATIVI (SOFTWARE)

a) I Servizi Informatici e Tecnologici provvedono all'acquisto delle licenze d'uso dei pacchetti applicativi necessari all'informatizzazione dell'Ente. Le caratteristiche del software applicativo acquistato sono definite dallo stesso Servizio sulla base delle esigenze degli utenti e della integrazione e compatibilità col SIC.

b) Le licenze d'uso dei pacchetti applicativi installati sono di proprietà del Comune.

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

d) L'utilizzo di tutti i programmi applicativi è limitato ai casi ed agli scopi previsti dall'Ente. 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 degli stessi.

f) Non è consentita l'esecuzione di alcuna modifica ai programmi applicativi se non, in casi particolari, dopo esplicita autorizzazione dell'Amministratore di Sistema. 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) È vietata la duplicazione o copia parziale del software installato nel SIC, con esclusione delle copie di salvataggio effettuate dall'Amministratore di Sistema.

i) È 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'Ente.

j) L'utente deve segnalare qualsiasi malfunzionamento od errore dei programmi applicativi in uso all' Amministratore di Sistema 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.

ART. 7
UTILIZZO DEL MATERIALE DI CONSUMO

a) I Servizi Informatici e Tecnologici provvedono all'acquisto di materiale di consumo (inchiostro, toner, supporti magnetici, supporti digitali, etc.), necessari per il funzionamento delle apparecchiature informatiche. Le caratteristiche del materiale di consumo acquistato sono definite dallo stesso Servizio sulla base delle esigenze degli utenti e della integrazione e compatibilità con le apparecchiature stesse. L'utilizzo di tale materiale è riservato esclusivamente ai compiti di natura strettamente istituzionale. Devono essere evitati in ogni modo sprechi dei suddetti materiali e/o utilizzi eccessivi.

ART. 8
GESTIONE INFORMATIZZATA DEL PERSONALE

La gestione informatizzata del personale avviene attraverso l'utilizzo di terminali che, rilevando le timbrature di ogni singolo dipendente, li invia, attraverso uno specifico software di gestione, ad apposito server che li elabora per renderli fruibili all'Ufficio Gestione Risorse Umane.
Il software permette:

a) la lettura dei transiti importati dai terminali, l'elaborazione delle assenze, delle presenze e delle maggiorazioni orarie. La produzione di stampe di base di cartellini, archivi ed esportazione dati per l'utilizzo con le procedure delle paghe.
b) la gestione dei flussi delle comunicazioni tra i dipendenti e l'ufficio Personale tramite INTERNET/INTRANET.

Il software, permette, inoltre, la gestione del "personale web", accedendo ad un apposito portale mediante autenticazione e nello specifico:

a) ai dipendenti di avviare uno scambio di informazioni con un "Ufficio Personale virtuale" per:
   - inserire i propri giustificativi;
   - inoltrare richieste di autorizzazione per ferie, permessi, straordinari, etc. (sia per un singolo giorno, che per un periodo o intervallo di tempo) che verranno inoltrate automaticamente ai responsabili ed in caso di approvazione, il sistema, in automatico, provvede a registrare la richiesta negli archivi del software di gestione presenze perché venga considerata nel normale ciclo di elaborazione (chiusura giornata, evidenza sulla lista presenti/assenti, etc.).
   - controllare in qualunque momento lo stato di avanzamento della richiesta;

- verificare "in tempo reale" le proprie timbrature sul cartellino presenze, le ferie residue, i permessi ancora disponibili, etc.

b) ai responsabili di settore di visualizzare le ferie, i permessi dei propri collaboratori in ogni momento ed in qualunque posto si trovino;

L'utilizzo a pieno della gestione informatizzata del personale, adeguerebbe sempre più l'Ente alla politica di innovazione tecnologica e dematerializzazione voluta dalle norme vigenti in materia.

Ai Servizi Informatici e Tecnologici spetta la gestione del software come amministratore di sistema (contatti con la ditta fornitrice del software, assegnazione password ai dipendenti, eventuali personalizzazioni del software, …), mentre, al Servizio Gestione Risorse Umane spetta il controllo e la lavorazione dei dati prodotti dal software.

ART. 9
GESTIONE DEGLI ARCHIVI

a) È buona prassi che le informazioni prodotte dagli utenti (documenti, archivi, dati in generale, ad esclusione dei documenti amministrativi generati dal sistema Sicr@web), siano memorizzate unicamente su cartelle predisposte sui dispositivi di rete (server) appositamente configurati dall'Amministratore di Sistema. Ciascun utente potrà accedere solamente ai dati contenuti all'interno della cartella (e sottocartelle) del Settore di appartenenza, salvo eccezioni dettate da esigenze organizzative. Scopo di queste cartelle è la creazione dell'archivio delle informazioni prodotte dagli utenti, nonché della "condivisione" delle informazioni tra gli utenti dello stesso Settore/Ufficio.

b) L'Amministratore di Sistema espleterà le attività volte a garantire la sicurezza delle informazioni memorizzate sui server di rete attraverso periodiche copie di salvataggio degli archivi.

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

d) Le informazioni eventualmente memorizzate sui dischi locali dei PC non sono protette e non vengono copiate durante l'esecuzione delle copie di salvataggio effettuate dal personale dei Servizi Informatici e Tecnologici. Gli utenti saranno responsabili della perdita dei dati eventualmente memorizzati su dispositivi locali rispondendo degli eventuali danni subiti dall'Ente.

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

f) Nel caso sia necessaria l'eliminazione di file per mancanza di spazio sui dischi di rete, tale operazione dovrà essere svolta con la supervisione dell'Amministratore di Sistema.

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

h) È vietata la copia di archivi contenenti dati personali su dispositivi amovibili (floppy disk, CD/DVD, USB pen drive nastri e simili) o su dispositivi di memorizzazione esterni all'Ente (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.

i) Il personale dei Servizi Informatici e Tecnologici, nell'ambito delle proprie attività di gestione e manutenzione del parco macchine, effettua controlli periodici sui PC 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 previa segnalazione al Responsabile di competenza, il quale provvederà a porre in atto eventuali provvedimenti disciplinari.

ART. 10
RISERVATEZZA DELLE INFORMAZIONI

a) Il SIC 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.

b) 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 SIC, ed in particolare ai dati personali, per i quali l'Ente assicura l'osservanza delle normative di legge.

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

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

e) Ogni utilizzatore del SIC possiede una propria e personale credenziale di autenticazione composta da un Identificativo Utente (UserID) e una Parola Chiave (Password) rilasciata dall' Amministratore di Sistema su richiesta del Responsabile di Settore. L'utente è responsabile della custodia delle credenziali e non è autorizzato per Legge a comunicarla a terzi.

f) L'utente può autonomamente modificare in qualsiasi momento la propria password. Egli è comunque obbligato dalle leggi vigenti a cambiarla almeno una volta ogni tre mesi e in caso di violazione della sua segretezza.
g) L'utente che desidera modificare la password in uso deve seguire le procedure indicate dall' Amministratore di Sistema.
h) I documenti riservati devono essere di norma custoditi su cartelle riservate dei server di rete.
i) È vietata la cifratura di documenti effettuata autonomamente dal dipendente se non in casi particolari e con l'autorizzazione del Responsabile del Settore al quale deve comunque essere consegnata copia della chiave di cifratura.
j) Ai sensi dell'Art.10 del Disciplinare tecnico allegato alla L.196/03, il Titolare e il Responsabile del Trattamento dati possono richiedere all'Amministratore di Sistema 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 di Sistema che la comunica al Titolare/Responsabile. L'Amministratore di Sistema che ha provveduto alla sostituzione della password comunica tempestivamente e per iscritto al dipendente l'avvenuto cambio delle credenziali di accesso e le motivazioni.
k) È buona norma utilizzare gli screen savers con blocco del PC tramite password.
l) L'utilizzo improprio della password, ad esempio per occultare documenti od errori commessi, è considerato illecito dall'Ente, che è eventualmente autorizzato a procedere nei confronti dell'utente ai sensi del C.C.N.L. e delle leggi vigenti.

ART. 11
CRITERI DI UTILIZZO DELLE APPARECCHIATURE TELEFONICHE

I Servizi Informatici e Tecnologici provvedono all'acquisto delle apparecchiature telefoniche necessarie per l'espletamento dell'attività dei dipendenti dell'Ente. La tipologia, la dotazione e la configurazione delle apparecchiature telefoniche sono definiti dallo stesso Servizio, sulla base delle esigenze degli utenti, su richiesta da parte del Responsabile del Settore di appartenenza e della integrazione e compatibilità con il SIC.

Utilizzo dei servizi e degli apparecchi telefonici

a) Fermo restando il rispetto dei principi e dei doveri di cui ai Capi precedenti, l'utilizzo delle utenze telefoniche di servizio per scopi personali è consentito solo in caso di urgenza, a fronte di occasionali ed improrogabili esigenze private.

b) Al fine di garantire un corretto utilizzo dei servizi di telefonia il Comune predispone, ove tecnicamente possibile, adeguate profilazioni che consentano l'effettuazione o meno delle diverse tipologie di chiamata.

c) Il Comune, per finalità di gestione contabile, procede alla registrazione e alla conservazione, per il tempo strettamente necessario, dei tabulati del traffico effettuato. Per motivi di privacy le ultime tre cifre delle numerazioni sono oscurate.

Disposizioni aggiuntive per la telefonia mobile

Fermo restando quanto espresso ai punti "a – b e c", la gestione della telefonia mobile avverrà a seguito di apposito regolamento.

a) È fatto assoluto divieto di cessione ai terzi degli apparecchi e delle SIM.

b) Se le condizioni tecniche lo consentono, i cellulari di servizio assegnati agli utenti devono risultare attivi e raggiungibili quando essi sono in attività di servizio.

c) Il traffico telefonico per ragioni di servizio deve essere attestato dal Responsabile del Settore assegnatario degli apparecchi di telefonia mobile, contestualmente alla consuntivazione periodica ivi prevista.

ART. 12
UTILIZZO DI INTERNET

a) L'Ente 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 all'Amministratore di Sistema dal Responsabile del Settore anche via mail.

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

d) L'Ente 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'Ente - nei siti visitati durante la navigazione, eccetto che per motivi strettamente legati alla propria attività e dopo esplicita autorizzazione del proprio Responsabile.

f) È tassativamente vietato il download (memorizzazione sul disco del proprio computer o su altri dispositivi di memorizzazione, anche rimovibili) di file 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 file da Internet, gli stessi devono essere immediatamente verificati con il software antivirus.

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

i) L'Ente 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 in base alle esigenze ed alle attività dei Settori. Tali esigenze sono segnalate per iscritto dai Responsabili di Settore interessati all'Amministratore di Sistema anche via mail.

j) L'Ente 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'Ente, 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.

ART. 13
UTILIZZO DELLA POSTA ELETTRONICA

f) L'Ente 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.).

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

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

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

j) 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.troina.en.it) e quindi la "personalità" dell'indirizzo non implica "privatezza" dello stesso.

k) I titolari di una casella di posta elettronica con un indirizzo riportante il proprio nominativo (es: gbianchi@comune.troina.en.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 secondo le seguenti specifiche:

   - **Nome Ufficio del Comune di Troina [mail istituzionale]**
     Questo messaggio e i suoi allegati sono indirizzati esclusivamente alle persone indicate. La diffusione, copia o qualsiasi altra azione derivante dalla conoscenza di queste informazioni sono rigorosamente vietate. Eventuali risposte a questo messaggio potranno essere conosciute nell'organizzazione di appartenenza del mittente. Qualora abbiate ricevuto questo documento per errore siete cortesemente pregati di dame immediata comunicazione al mittente e di provvedere alla sua distruzione. Grazie.

l) La creazione di un nuovo indirizzo di posta elettronica deve essere richiesto dal Responsabile del Settore per iscritto all'Amministratore di Sistema anche via mail, specificando il nominativo del dipendente cui è assegnato (referente).

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

n) 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.

o) 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.

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

ART. 14
ASSISTENZA E SERVIZI

Procedure operative

Al fine di rendere possibile la gestione, con elevata semplicità, efficienza e funzionalità, del parco macchine dell'Ente, gestendole sia dal punto di vista hardware che software, anche in presenza di riorganizzazioni degli uffici, l'Ente si è dotato di un applicativo denominato OSACed.

OSACed consente al personale dei Servizi Informatici e Tecnologici, di ottimizzare e ridurre i costi per le risorse ICT attraverso il recupero di componenti hardware e/o di licenze software ancora valide. Attraverso l'installazione su ogni PC dell'Ente di apposito "Agent", censisce e monitora, in maniera costante e aggiornata, il parco informatico locale e/o remoto in gestione. Ovvero, individua automaticamente tutti i dispositivi collegati in rete rilevandone la configurazione hardware e software. Monitora e traccia automaticamente le variazioni rilevate, consente di conoscere tutti i software ed i componenti HW presenti in ciascun PC, oltre alla loro esatta ubicazione (ufficio) e la persona/e che opera sugli stessi (riferimenti), *(Propedeutico per i controlli inerenti l'art. 171–bis, comma 1, L. 633/1941, modificato dalla L. 248/2000 Duplicazione ed altre azioni illecite su programmi per elaboratore e su banche dati).* Aiuta il personale dei Servizi Informatici e Tecnologici nelle funzioni operative quali ad esempio la gestione PC in remoto con diagnosi e risoluzione dei problemi e lancio di patch e aggiornamenti. Semplifica e ottimizza, la gestione delle richieste di intervento tecnico (via telefono e via web) da parte degli utenti. Crea automaticamente le commesse di lavoro, rapportini di intervento ecc…..

Attraverso un apposito modulo, *"Trouble ticketing"*, gestisce le richieste di intervento da parte di tutto il Personale utente, garantendo la tracciabilità delle richieste, la creazione automatica delle relative commesse di intervento ed il monitoraggio delle ore/tempo di lavoro impiegate sia per gli

interventi eseguiti dal servizio informatico, che per quelli affidati in outsourcing (ad es. Aziende esterne).

a) Le procedure operative per le richieste di assistenza/servizi di cui al punto "b" sono regolate da apposita procedura di gestione delle richieste (Web Ticketing).

b) Il Web Ticketing istruisce le principali richieste di assistenza/servizio, ovvero:
   - richiesta di acquisto, sostituzione o spostamento di un PC, stampante, scanner e altre apparecchiature;
   - richiesta di abilitazione all'accesso alla rete Internet;
   - richiesta di creazione del profilo di posta elettronica e abilitazione all'accesso della casella di posta elettronica dell'ufficio;
   - richiesta di accesso alle informazioni presenti nelle cartelle condivise d'ufficio;
   - richiesta di creazione, modifica e cancellazione di un'utenza per l'accesso ai servizi della rete comunale;
   - prenotazione per il prestito di un apparato multimediale (personal computer e proiettore);
   - richiesta di installazione di un nuovo applicativo;
   - richiesta di abilitazione ai servizi erogati sulla Intranet comunale per l'accesso a banche dati esterne;
   - richiesta di abilitazione ai servizi erogati sulla Intranet comunale per l'accesso a banche dati interne (Anagrafe, Protocollo, e altri servizi);
   - richiesta di ripristino del PC, stampante o altro dispositivo fornito dall'ente;
   - richiesta di ripristino del funzionamento di software e programmi applicativi installati dall'Ente.

c) Il Dipendente apre un «Ticket», che scaturisce in prima battuta nella segnalazione al personale dei Servizi Informatici e Tecnologici, che valuta la richiesta pervenuta. A seconda del tipo di richiesta, il Responsabile dei Servizi Informatici e Tecnologici chiederà parere al Responsabile del Settore di pertinenza del dipendente. Se viene respinta, il Responsabile dei Servizi Informatici e Tecnologici ne dà comunicazione all'utente; se viene approvata, passerà per la valutazione tecnica. In caso di valutazione positiva l'attività verrà espletata dandone comunicazione al dipendente e al Responsabile di Settore.

d) Per tutti gli interventi di ripristino del funzionamento di un PC, o di una stampante, nonché dei programmi e dell'impiego degli apparati multimediali (in dotazione all'Ente) non è necessaria l'autorizzazione del Responsabile di Settore.

e) La presa in carico delle richieste di cui al punto "b" non è garantita qualora non venga rispettato l'iter descritto ai punti "a" e "c" del presente articolo.

ART. 15
PROTEZIONE ANTIVIRUS

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

g) Il software antivirus installato su un server di rete, verrà aggiornato in modo automatico secondo le procedure definite dall'Amministratore di Sistema.

h) 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.

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

j) Ogni dispositivo magnetico di provenienza esterna all'Ente dovrà essere verificato mediante il programma antivirus prima del suo utilizzo, e, nel caso in cui venissero rilevati virus, non dovrà essere utilizzato.

ART. 16
ACCESSO AD ARCHIVI CONTENENTI DATI PERSONALI (D.LGS. 196/03 "CODICE SULLA PRIVACY")

a) Il Comune di Troina, 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 Responsabili di Settore ognuno per gli archivi di propria competenza.

b) 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.

c) 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.

d) All'atto della nomina, gli Incaricati del trattamento riceveranno precise indicazioni sul tipo di trattamento dei dati che sarà loro consentito.

e) 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.

f) 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 ("logout" o "chiudi sessione").

ART. 17

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

a) Le politiche 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.

b) L'Ente, nella gestione del SIC, 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 che 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.

c) Il SIC ed in particolare quello preposto 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).

d) I controlli effettuati dall'Ente 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 reati 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".

e) 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'Ente possono riguardare altre informazioni che sono sempre trattate secondo i principi di pertinenza e non eccedenza.

f) La custodia delle informazioni tecniche (log monitoraggio) riguardanti l'utilizzo dei sistemi è assicurato dal Responsabile del Trattamento dati e/o dal Responsabile dei Servizi Informatici e Tecnologici che previene qualsiasi accesso illecito a tali dati. A tal proposito sono adottate adeguate misure di sicurezza informatica.

ART. 18
SISTEMA DI VIDEOSORVEGLIANZA

Il sistema di videosorveglianza prevede una rete di telecamere per il controllo delle aree più significative del territorio del Comune. La centrale operativa, predisposta nella sede della Polizia Municipale, ha il compito di visualizzare i punti di ripresa. Sono gestiti dal responsabile della gestione tecnica degli impianti di videosorveglianza designato dal Sindaco.

La nomina del responsabile della gestione tecnica è effettuata con decreto del Sindaco, nel quale sono analiticamente specificati i compiti affidati allo stesso. Il Responsabile, così come individuato dal Sindaco, nella qualità di responsabile della gestione tecnica degli impianti di videosorveglianza:

a) cura l'installazione e gestisce la manutenzione degli impianti di videosorveglianza;

b) assegna e custodisce le credenziali di accesso necessarie per l'utilizzo degli impianti di videosorveglianza;

c) cura e gestisce i rapporti con le Aziende esterne incaricate per la installazione e manutenzione dei suddetti apparati.

Per tutto quanto attiene alla regolamentazione del Sistema di Videosorveglianza, si rinvia integralmente alle disposizioni contenute nel *"Regolamento per l'utilizzazione degli impianti di videosorveglianza del Comune di Troina"* approvato con Delibera del Consiglio Comunale n. 40 del 10/04/2015.

ART. 19
INSTALLAZIONE DI SISTEMA DI PONTI RADIO TIPO HIPERLAN, WI-FI o WI-MAX

Al fine di garantire la diffusione di uno o più servizi, anche di comunicazione tramite banda larga, dedicati alla cittadinanza ed alle realtà produttive locali, l'Ente consente l'istallazione di sistema di ponti radio a bassa emissione elettromagnetica (di tipo HiperLAN, Wi-Fi o Wi-Max) necessari all'acquisizione/trasmissione del segnale sui tetti degli edifici comunali compreso il Municipio – sede centrale di Via Conte Ruggero, in grado di coprire anche le parti del territorio non coperte con l'utilizzo delle più moderne tecnologie.

Tali apparati rappresentano un vantaggio notevole per il cittadino che potrà scegliere, fra le diverse opzioni, di poter usufruire di un collegamento internet effettivamente adeguato alle esigenze di velocità nell'acquisizione/trasferimento dei dati.

L'installazione, il mantenimento, il funzionamento, l'esercizio, la mera innovazione tecnologica ed adeguamento degli impianti è a carico dei richiedenti.

L'Amministrazione non è responsabile per la custodia degli impianti.

I richiedenti, a propria cura, responsabilità e spese, si faranno carico di tutti gli interventi e lavori per rendere l'immobile idoneo allo scopo per il quale viene concesso **previa apposita domanda da inoltrare al Responsabile del IV Settore "Urbanistica-Edilizia" e al Responsabile dei Servizi Informatici e Tecnologici, che dovrà esprimere parere per il rilascio della necessaria autorizzazione a seguito di stipula di apposita convenzione. Sarà altresì, a carico dei richiedenti l'ottenimento di eventuali ulteriori** concessioni, autorizzazioni e nulla-osta necessari all'installazione dell'impianto.

I lavori di installazione dovranno essere eseguiti a perfetta regola d'arte, in particolare per quanto riguarda l'integrità, in generale, e gli aspetti strutturali, in particolare, del fabbricato che delle antenne e loro supporti, in ottemperanza a tutte le norme vigenti ed **all'autorizzazione rilasciata dal Responsabile del IV Settore previo parere del Responsabile dei Servizi Informatici e Tecnologici**.

Il rilascio di Autorizzazione non attribuisce alcun diritto di esclusiva al concessionario per cui potranno installarsi altri operatori.

Le concessionarie, se non previsto da apposita norma di Legge, dovranno versare al Concedente un canone annuo pari a € 200,00 per una superficie di proiezione pari a mq. 1 e di € 500,00 per una superficie di proiezione superiore a mq. 1. Il suddetto canone sarà comunicato alle concessionarie subito dopo l'assenso per il rilascio della relativa autorizzazione.

A seguito di accordo con l'Ente, in sostituzione del canone le concessionarie forniranno:

- n. 5 hotspot in luogo del canone di € 200,00;
- n. 10 hotspot in luogo del canone di € 500,00.

Gli hotspot dovranno essere posizionati in luoghi stabiliti dall'Ente.

Le concessionarie dovranno mantenere il manufatto, e tutte le altre opere dalla stessa realizzate, in perfetto stato e dovranno immediatamente riparare ogni danno che si verificasse alla struttura, sotto la comminatoria, in caso di inadempienza di tali obblighi, dell'esecuzione d'ufficio a suo carico. Se necessario, in particolare ai fini di eventuali manutenzioni atte a garantire l'adeguamento statico del manufatto, le ditte concessionarie si impegnano, con ogni spesa ed onere a proprio carico, a trasferire in traliccio temporaneo i propri apparati fino a ripristino delle condizioni di operatività. Al termine di tali manutenzioni le ditte concessionarie potranno riposizionare le antenne secondo le precedenti modalità installative, o concordando nuove modalità di installazione laddove opportuno o necessario.

Al termine della concessione o in caso di recesso o di risoluzione, le concessionarie provvederanno a propria cura e spese, nei tempi tecnici necessari ma, in ogni caso, non oltre giorni 90 (novanta), a rimuovere quanto da essa installato e alla rimessione dell'immobile in pristino. Decorso inutilmente tale termine e previa diffida scritta della Concedente, quest'ultima avrà facoltà di ordinare e far eseguire d'ufficio, a spese della Concessionaria, la rimozione delle opere installate. Fino alla suddetta rimozione ogni responsabilità connessa all'impianto rimane a carico della Concessionaria.

La concessione viene data senza pregiudizio di terzi, verso i quali la Concessionaria assume ogni responsabilità, rimanendo obbligata a tenere indenni e sollevati i concedenti da ogni azione molesta, danni e spese che potessero per qualsiasi motivo essere cagionate dalla concessione stessa.

La Concessionaria garantisce che le proprie apparecchiature installate sugli immobili di proprietà comunale sono conformi alle leggi vigenti in materia e non provocheranno alcun tipo di disturbo alla salute del cittadino. Esonera e solleva espressamente la Concedente da qualsiasi responsabilità, danno, spesa, gravame o molestia che a quest'ultima, a terzi o ad apparati elettronici di informatica, di telefonia e televisivi degli edifici circostanti, potessero derivare a causa o per l'effetto dell'installazione, e del funzionamento dell'impianto.

La Concedente, al fine di veicolare dati e fonia con le varie sedi periferiche, potrà far installare ulteriori apparati senza comunicazione alle varie concessionarie già autorizzate. Stante la possibilità di interferenze reciproche fra apparecchiature non gestite nell'ambito di un progetto unitario, volto alla diffusione di uno o più servizi dedicati alla cittadinanza del comune, alle realtà produttive locali, ai servizi che eroga l'Ente, ed al fine di impedire l'insorgere di malfunzionamenti alle apparecchiature gestite da terzi per conto della Concedente, nei medesimi locali e/o comunque nell'ambito del medesimo stabile, la Concedente informa l'Operatore che fornisce i servizi telematici per conto della stessa, almeno 15 (quindici) giorni prima del rilascio di nuova concessione, allegando il materiale tecnico necessario all'analisi ed alla valutazione di compatibilità e la stessa **dovrà far conoscere il parere tecnico di compatibilità entro i successivi 15 giorni.**

Detto parere non è vincolante per il Concedente ma, in caso di incompatibilità con i servizi dell'Ente, lo stesso potrà non fare installare ulteriori apparecchiature.

Qualsiasi variazione alle modalità di occupazione e/o all'estensione della superficie occupata è soggetta al preventivo rilascio, a seconda dei casi, o di nuova concessione o di semplice benestare scritto.

La concessionaria si impegna ad adottare tutti gli accorgimenti necessari ed opportuni per non recare danno all'immobile o alle apparecchiature in esso contenute e solleva la Concedente da ogni responsabilità per gli eventuali danni che a chiunque possano derivare dalla custodia e/o a causa dell'utilizzo dell'immobile e dell'impianto da parte della stessa.

La Concessionaria, direttamente o a mezzo di personale da essa incaricato, avrà facoltà di accedere agli immobili con le modalità sotto indicate, in ogni momento, ventiquattr'ore su ventiquattro, festività comprese, per effettuare tutti gli interventi relativi alla installazione, conduzione, manutenzione e controllo dell'impianto impegnandosi in ogni modo a recare il minor disagio possibile alla Concedente ed a terzi, dandone comunicazione al Responsabile dei Servizi Informatici e Tecnologici dell'Ente. **Qualora per l'effettuazione di tali interventi, si rendesse necessario accedere ai locali dell'edificio che ospita l'attrezzatura, tale accesso dovrà avvenire alla presenza di personale autorizzato dal Concedente attraverso il Responsabile dei Servizi Informatici e Tecnologici dell'Ente.**

La convenzione da stipulare con la Concessionaria è subordinata alla predisposizione da parte della stessa di idonea copertura assicurativa, con primaria Compagnia di Assicurazione, per danni a persone e cose arrecabili in qualsivoglia modo dall'impianto che verrà installato. Copia integrale della citata polizza, che potrà avere anche carattere generale e non riferimento specifico all'impianto, purché quest'ultimo risulti coperto dalle condizioni di tale polizza generale, dovrà essere consegnata entro 20 giorni dalla data di stipula della convenzione.

Sono fatti salvi gli apparati installati precedentemente all'approvazione del presente regolamento, che, al fine di impedire l'insorgere di malfunzionamenti alle apparecchiature gestite da terzi per conto della Concedente, potranno essere sottoposti a verifica di compatibilità. In ogni caso dovranno predisporre idonea copertura assicurativa da consegnare all'Ente entro i termini stabiliti da apposita richiesta da emanarsi entro 60 giorni dall'approvazione del Regolamento.

Le spese tutte, inerenti e conseguenti alla convenzione, saranno a carico della Concessionaria che dovrà dichiarare espressamente di assumerle (comprese quelle per la registrazione e dei rinnovi, nonché l'IVA, l'imposta di registro e di bollo).

Nel caso in cui **la concessionaria** o una delle Parti addivenga a fusioni, cessioni parziali o totali dell'attività o ad eventuale altra modifica della denominazione sociale, anche eventualmente conseguente ad accordi di area o programmatici con Enti equivalenti, la concessione potrà essere ceduta quale conseguenza di tale atto, previo comunicazione scritta alla controparte, restando invariati termini e condizioni della medesima.

ART. 20
FORMAZIONE E AGGIORNAMENTO

Il Comune di Troina promuove, all'interno del piano annuale della formazione, l'aggiornamento e la formazione dei propri dipendenti in merito al corretto utilizzo delle strumentazioni informatiche e delle apparecchiature telefoniche.

ART. 21
INFORMATIVA

Ai sensi dell'art. 13 del D.lgs n. 196 del 30 giugno 2003 si comunica che:

a) l'Amministratore di sistema, può effettuare il trattamento dei dati relativi al traffico sulla rete;
b) il titolare dei dati di traffico è il Sindaco;
c) la presa visione e l'accettazione delle condizioni contenute nel presente regolamento costituiscono l'informativa e l'esplicito consenso da parte dell'utente alla raccolta ed all'eventuale trattamento dei dati relativi al traffico.

In ogni caso i sistemi informatici 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".

Il presente Regolamento, è stato, prima della sua diffusione tra tutti gli utilizzatori di strumenti informatici e telematici messo a disposizione dall'Amministrazione comunale, oggetto, ai sensi dell'art. 4, comma 2, della legge n.300/1970, di previo accordo con le rappresentanze Sindacali dei

lavoratori. Esso viene diffuso tra i dipendenti del Comune di Troina e adeguatamente pubblicizzato, oltre che nel sito web del Comune, a tutti gli utenti che facciano utilizzo di risorse strumentali informatiche dell'Ente.

I Responsabili dei Settori/Servizi/Uffici sono tenuti a vigilare affinché le presenti disposizioni siano comunicate a tutti gli utilizzatori delle risorse informatiche dell'Ente.

Inoltre, il dipendente deve attenersi, nell'utilizzo e nella gestione delle risorse strumentali informatiche comunali, ai principi e ai doveri contenuti nel "Codice di comportamento dei dipendenti delle pubbliche amministrazioni" di cui al Decreto Ministero Funzione Pubblica del 28/11/2000.

I documenti sopra richiamati (Deliberazione del Garante Privacy n.13/2007, D.M. della Funzione Pubblica del 28/11/2000 e Direttiva n.02/09 del Dipartimento della Funzione Pubblica) possono essere reperiti ai seguenti indirizzi internet:

http://www.garanteprivacy.it/garante/doc.jsp?ID=1387522

http://bancadati.digita-lex.it

ART. 22

PRESA VISIONE ED ACCETTAZIONE DEL REGOLAMENTO

Il sottoscritto/a _____

Nato/a _____

Residente _____ in via_____

Telefono _____ cod. fisc. _____

Dichiara di:

- aver preso visione ed accettare tutte le norme contenute nel regolamento d'uso del sistema Informativo del Comune di Troina;
- aver acquisito le informazioni di cui all'art. 13 del D.lgs n. 196 del 30 Giugno 2003;
- essere a conoscenza dei diritti dell'interessato di cui agli articoli 7, 8, 9, 10, del medesimo decreto.

Data _____ Firma _____

ART. 23

ENTRATA IN VIGORE

Il presente regolamento entra in vigore decorsi 15 giorni dalla sua pubblicazione.

ALLEGATO A

GLOSSARIO DEI TERMINI TECNICI E INFORMATICI

Account	Iscrizione registrata su un server e che, tramite l'inserimento di una user id e di una password, consente l'accesso alla rete e/o ai servizi. Ad esempio, un account ci permette di entrare in Internet, un altro account ci serve per ricevere e spedire posta elettronica. Un account ci consente di accedere alle risorse di una rete locale, come server, file server, stampanti. Altri account servono per accedere a server e servizi vari.
Amministratore di Sistema	Figura essenziale per la sicurezza delle banche dati e la corretta gestione delle reti telematiche. È chiamato a svolgere delicate funzioni che comportano la concreta capacità di accedere a tutti i dati che transitano sulle reti aziendali ed istituzionali. Ad esso viene affidato spesso anche il compito di vigilare sul corretto utilizzo dei sistemi informatici di un'azienda o di una pubblica amministrazione.
Antivirus	Tipo di software che cerca e distrugge gli eventuali virus e cerca di rimediare ai danni che hanno compiuto.
Backup	Termine, che significa copia di sicurezza, indica l'operazione di duplicare su differenti supporti di memoria le informazioni (dati o programmi) presenti sui dischi di una stazione di lavoro o di un server. Normalmente viene svolta con una periodicità stabilita.
Chat	(letteralmente, "chiacchierata") è un servizio informatico che permette attraverso internet, di attivare e gestire un dialogo in tempo reale fra due o più utenti utilizzando principalmente messaggi testuali.
Database	(Base di Dati). Qualsiasi aggregato di dati organizzato in campo (colonne) e record (righe).
Dati giudiziari	I dati giudiziari sono quei dati personali in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti. Inoltre possono essere quei dati personali indicanti la qualità di imputato o di indagato.
Dati personali	(art. 4 c. 1 lett b) del D.lgs. 196/03) identificano le informazioni relative alla persona fisica, giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altro dato, ivi compreso un numero di riconoscimento personale.
Dati sensibili	secondo il Codice sulla protezione dei dati personali (d.lgs. 196/2003), art.4, sono considerati dati sensibili, e dunque la loro raccolta e trattamento sono soggetti sia al consenso dell'interessato sia all'autorizzazione preventiva del Garante per la protezione dei dati personali (art. 26), i dati personali, idonei a rivelare: •l'origine razziale ed etnica, •le convinzioni religiose, filosofiche o di altro genere, •le opinioni politiche, •l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, •lo stato di salute e la vita sessuale
Download	Registrare sul proprio disco rigido un file richiamandolo, tramite modem o rete, da un computer, da un server o da un host (tramite Internet, rete locale o geografica).
E-mail	Electronic mail, posta elettronica. Scambio di messaggi e di file attraverso una rete locale o Internet. Avviene in tempo reale ed è indipendente dalla

	posizione fisica dei computer mittente e destinatario. I messaggi e file vengono conservati da un server che provvede ad inoltrarli al destinatario quando questo si collega.
Firewall	Insieme di software/hardware usato per filtrare i dati in scambio fra reti diverse, al fine di proteggere un server da attacchi pervenuti via rete locale o via Internet. Consente il passaggio solamente di determinati tipi di dati, da determinati terminali e determinati utenti.
Hardware	Letteralmente ferramenta, in informatica si intende l'insieme dei componenti (CPU, Hard Disk ecc.) che costituiscono un computer.
ID utente	Codice identificativo personale per l'accesso ai sistemi informatici. Normalmente è formato dall'iniziale del nome.cognome.
Internet	La madre di tutte le reti di computer. E' l'insieme mondiale delle reti di computer interconnesse.
Intranet	Rete locale che, pur non essendo necessariamente accessibile dall'esterno, fa uso di tecnologie Internet.
Guestbook	(libro degli ospiti) è un'utilità interattiva che permette ai visitatori di un sito web di poter lasciare traccia delle navigazioni.
Log	Termine, che significa giornale di bordo o semplicemente giornale, viene utilizzato nell'informatica per indicare la registrazione cronologica delle operazioni man mano che vengono eseguite ed il file su cui tali registrazioni sono memorizzate.
Password	(in italiano: "parola chiave", "parola d'ordine", o anche "parola d'accesso") è una sequenza di caratteri utilizzata per accedere ad una risorsa informatica.
PC	**personal computer** (espressione inglese che significa letteralmente "calcolatore personale"), solitamente abbreviato in **PC**, è un qualsiasi computer di uso generico le cui dimensioni, prestazioni e prezzo di acquisto lo rendono adatto alle esigenze del singolo individuo nell'uso quotidiano.
Principio di necessità	è un principio generale dell'ordinamento che presiede all'adozione di tutte le misure straordinarie da parte delle Autorità.
SIC	Il sistema informativo comunale è l'insieme di componenti interconnessi atti a raccogliere, elaborare, memorizzare e diffondere informazioni al fine di supportare il processo decisionale, il coordinamento, il controllo e l'analisi e la visualizzazione in un'organizzazione.
Software freeware	Software freeware: Programmi software distribuiti in modo gratuito.
Software peer-to-peer	Programmi utilizzati per la condivisione e lo scambio di files fra elaboratori. Questi programmi vengono utilizzati principalmente per scambiarsi file di tipo mp3, (file musicali) e DivX (contenenti film) spesso in violazione dei diritti d'autore.
Stand-alone	Si riferisce ad un'apparecchiatura capace di funzionare da sola, indipendentemente dalla presenza di altre apparecchiature con cui potrebbe comunque interagire.
User Id	Nome utente
Utente (User)	Chiunque utilizzi un elaboratore collegato alla rete, sia che il collegamento avvenga in rete locale sia che si tratti di un accesso remoto.
Unità di rete	Spazio disco condiviso che risiede fisicamente su altro computer o server
Virus	Programma creato per diffondersi da computer a computer, spesso danneggiando i dati e gli altri programmi.