

**REGOLAMENTO PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI, DELLA POSTA ELETTRONICA
E DI INTERNET**

SOMMARIO 23 dicembre 2017

Art. 01 Finalità	Pg. 02
Art. 02 Principi generali	Pg. 02
Art. 03 Ambito di applicazione	Pg. 02
Art. 04 Soggetti autorizzati all'utilizzo del sistema informativo comunale	Pg. 03
Art. 05 Titolarità degli strumenti e delle apparecchiature informatiche	Pg. 03
Art. 06 Rispetto della proprietà intellettuale e delle licenze	Pg. 04
Art. 07 Criteri Generali	Pg. 04
Art. 08 Sicurezza del sistema informativo comunale	Pg. 05
Art. 09 Utilizzo dei dati e del software	Pg. 06
Art. 10 Gestione delle credenziali d'accesso	Pg. 06
Art. 11 Modalità di utilizzo degli strumenti informatici	Pg. 07
Art. 12 Uso di supporti removibili	Pg. 09
Art. 13 Gestione degli accessi alla rete comunale	Pg. 09
Art. 14 Postazioni di lavoro (PDL)	Pg. 10
Art. 15 Assistenza su PDL	Pg. 10
Art. 16 Utilizzo della Posta Elettronica	Pg. 11
Art. 17 Utilizzo di Internet	Pg. 13
Art. 18 Monitoraggio e controlli	Pg. 15
Art. 19 Violazioni	Pg. 15
Art. 20 Norme finali	Pg. 15

Art. 01 – Finalità

1. Il presente regolamento è diretto a definire le modalità di accesso ed utilizzo, da parte degli amministratori, dei dipendenti e dei collaboratori del Comune Tarquinia, degli strumenti informatici, di Internet e della posta elettronica nell'ambito dello svolgimento delle proprie mansioni e compiti, ai fini di un corretto utilizzo degli strumenti stessi.
2. Il Comune di Tarquinia adotta ogni opportuna misura, organizzativa e tecnologica, volta a prevenire il rischio di utilizzi impropri delle strumentazioni e delle banche dati di proprietà dell'Ente e disciplina le modalità con cui effettuerà i relativi controlli.
3. Considerato che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza (Decreto del Presidente della Repubblica del 16 Aprile 2013, n. 62), il presente regolamento è diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.

Art. 02 - Principi generali

1. Il Comune di Tarquinia promuove l'utilizzo degli strumenti informatici, di Internet e della posta elettronica quali mezzi utili a perseguire con efficacia ed efficienza le proprie finalità istituzionali, in accordo con le linee guida e i principi delineati dalla normativa vigente.
2. Ogni utente è responsabile, civilmente e penalmente, del corretto uso delle risorse informatiche assegnate, con particolare riferimento alle dotazioni tecniche ed ai servizi al cui utilizzo è autorizzato nonché ai dati trattati a fini istituzionali. E' altresì responsabile del contenuto delle comunicazioni effettuate e ricevute a fini istituzionali anche per quanto attiene la riservatezza dei dati ivi contenuti, la cui diffusione impropria potrebbe configurare violazione del segreto d'ufficio o della normativa per la tutela dei dati personali. Sono vietati comportamenti che possono creare un danno, anche di immagine all'Ente.
3. L'utente, pertanto
 - a) deve custodire con cura ed utilizzare in modo appropriato gli strumenti informatici hardware e software che gli vengono assegnati, evitando manomissioni, danneggiamenti o utilizzi, anche da parte di altre persone, per scopi non consentiti;
 - b) risponde del diligente uso di Internet e della posta elettronica;
 - c) è responsabile della propria postazione di lavoro.

Art. 03 – Ambito di applicazione

1. Il sistema informativo comunale è costituito dall'insieme delle risorse informatiche, cioè dalle risorse infrastrutturali e dal patrimonio informativo digitale.

2. 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.
3. La presente disciplina individua regole comuni per tutelare i reciproci diritti e doveri degli utenti e dell'Amministrazione attraverso la definizione:
- delle modalità per l'utilizzo e l'accesso al servizio Internet e di posta elettronica da parte dei soggetti che a vario titolo prestano servizio o attività per conto e nelle strutture del Comune;
 - del diritto dell'Amministrazione di verificare che non si verifichino usi impropri;
 - del diritto del lavoratore (e dei terzi) ad una sfera di riservatezza anche nelle relazioni lavorative.
4. Le prescrizioni contenute si aggiungono e integrano le norme già previste dal contratto collettivo nazionale di lavoro, nonché dalla normativa in materia di protezione dei dati personali D.Lgs. 196/2003.

Art. 04 – Autorizzazioni all'utilizzo del sistema informativo comunale

1. Le autorizzazioni all'utilizzo del sistema informativo comunale sono assegnate in funzione del ruolo degli amministratori comunali e della collocazione di ogni dipendente comunale nell'organigramma dell'ente sulla base delle relative esigenze operative.
2. Il personale dipendente autorizzato all'utilizzo delle risorse informatiche è individuato dal Responsabile di ciascun Settore in sede di definizione delle mansioni operative attribuite ed è, di norma, quello destinato all'espletamento di attività amministrative e/o tecniche.
3. Il personale delle società ospitate nei locali dell'ente, delle forze di polizia, di altri enti pubblici o di società esterne può accedere ai servizi del sistema informativo comunale previa stipula di apposita convenzione con l'Ente. Le richieste di autorizzazione all'accesso devono essere trasmesse dai responsabili delle strutture esterne all'Amministratore di sistema. Detto personale è a tutti gli effetti un utente del sistema informativo comunale ed è soggetto al presente regolamento.
4. Il personale esterno incaricato dall'ente (es. consulenti, stagisti, personale interinale) può accedere ai servizi del sistema informativo comunale previa richiesta di autorizzazione all'accesso che deve essere trasmessa dal competente Responsabile di Settore all'Amministratore di sistema. Il personale esterno incaricato e autorizzato dall'Ente è a tutti gli effetti un utente del sistema informativo comunale ed è soggetto al presente regolamento.
5. Il personale dipendente, nonché i collaboratori, possono essere autorizzati, dall'Ufficio Sistema Informativo Comunale (da ora SIC) su richiesta del Responsabile del Settore nel quale l'utilizzatore è inquadrato ovvero nell'interesse del quale effettua la propria prestazione, ad avvalersi di personal computer "portatili" sia presso i locali a disposizione dell'Amministrazione Comunale, sia in occasione di missioni o trasferte, qualora necessario ed indispensabile allo svolgimento dell'attività lavorativa.

Art. 05 – Titolarità degli strumenti e delle apparecchiature informatiche

1. Il Comune di Tarquinia è proprietario degli strumenti e delle apparecchiature informatiche assegnate ai dipendenti o collaboratori e di tutti i documenti prodotti dagli utenti e memorizzati nell'hardware di proprietà del Comune e/o negli storage a cui afferiscono i programmi gestionali operanti in cloud.

Art. 06 - Rispetto della proprietà intellettuale e delle licenze

1. Tutti gli utenti sono tenuti al rispetto delle leggi in materia di tutela della proprietà intellettuale (copyright).
2. Tutto il software in uso per il funzionamento dei servizi e degli uffici per cui sia prevista una licenza d'uso deve essere ottenuto seguendo le procedure di acquisizione definite dai regolamenti comunali e deve essere registrato a nome del Comune di Tarquinia.
3. Tutto il software che non richieda una licenza d'uso a titolo oneroso, quale il software a sorgente aperto (open source) o il software distribuito con licenza d'uso di tipo freeware o shareware, deve essere selezionato e reso disponibile per gli utenti dall'Ufficio SIC, competente per la materia.
4. NON è consentito installare, sulle apparecchiature fornite, qualsivoglia hardware o software, né duplicare o utilizzare software che non sia stato preinstallato, installato o comunque fornito dall'Amministrazione Comunale tramite l'Ufficio SIC al fine di evitare il grave pericolo di introdurre virus informatici nel sistema informativo comunale; per quanto riguarda il software autorizzato si fa riferimento all'elenco previsto dal "Regolamento sull'applicazione delle Misure Minime di Sicurezza I.C.T. – controllo ABSC2-Inventario dei software autorizzati e non autorizzati".
5. L'installazione di componenti software in grado di danneggiare il sistema informativo o le informazioni in esso contenute costituisce illecito disciplinare e può costituire condotta sanzionata anche penalmente, ai sensi dell'art. 635 bis del codice penale (Danneggiamento di sistemi informatici e telematici).

Art. 07 - Criteri generali

1. Tutto l'hardware ed il software in dotazione agli uffici deve essere acquisito nel rispetto delle specifiche tecniche fornite dall'Ufficio SIC, competente per la materia.
2. L'utilizzo delle stampanti e dei materiali di consumo in genere (carta, inchiostro, toner, supporti magnetici, supporti digitali) è riservato esclusivamente per lo svolgimento di compiti di natura strettamente istituzionale; devono essere evitati in ogni modo sprechi o utilizzi eccessivi dei suddetti materiali.
3. L'utente avrà cura di effettuare la stampa di documenti contenenti "dati personali" solo se strettamente necessaria provvedendo a ritirarli immediatamente dai vassoi delle stampanti condivise.
4. Si dovrà limitare per quanto possibile, di dislocare stampanti e fax in aree accessibili a soggetti non abilitati al trattamento e non presidiate (per esempio: corridoi aperti al pubblico, sale d'attesa, ecc.).
5. L'Amministrazione comunale ed i Responsabili dei Settori si impegnano a ridurre ovvero ad eliminare, ove possibile, l'utilizzo da parte degli utenti di stampanti e/o di scanner personali in favore di dispositivi compartimentali (o di piano), che permettono un risparmio nei costi di gestione; le stampanti e gli scanner ad uso individuale dovranno quindi essere riservati esclusivamente ad utilizzo sporadico/di emergenza.

6. Tutte le stampanti multifunzione di rete, i plotter e stampanti laser messe a disposizione dall'Ufficio SIC, indipendentemente dalla collocazione negli uffici e geografica, sono a disposizione di tutti gli utenti che, per esigenze di servizio, debbano utilizzarli.

Art. 08 - Sicurezza del sistema informativo comunale

1. Al fine di proteggere l'integrità del sistema informativo comunale, il Comune di Tarquinia si è dotato di:

- (a) apparati di sicurezza perimetrale che possono limitare la visibilità di siti web o servizi esterni e prevedere l'analisi del traffico da/verso Internet;
- (b) sistema antivirus centralizzato che protegge tutte le macchine in uso presso i vari servizi ed uffici.

2. L'antivirus è installato su ogni postazione di lavoro a cura dell'Ufficio SIC ed il suo aggiornamento avviene in maniera automatica.

3. Nel caso che il software antivirus rilevi la presenza di un virus che non sia riuscito a ripulire, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer e segnalare l'accaduto al personale incaricato dell'Ufficio SIC; stessa cosa qualora noti comportamenti anomali quali esecuzione automatica di programmi, alterazione di file etc.

4. L'utente è tenuto ad osservare tutte le prescrizioni fornite dall'Ufficio SIC al fine di evitare infezioni e installazione di software malevolo; in particolare:

- a) NON utilizzare supporti removibili (per es. chiavette/dischi esterni USB) senza aver prima effettuato una scansione degli stessi tramite antivirus;
- b) NON aprire allegati o visitare link contenuti in e-mail di dubbia provenienza; nel caso si abbiano dubbi in merito contattare preventivamente il SIC;
- c) NON connettere postazioni di lavoro o apparati personali alle reti LAN e Wireless dell'Ente senza aver fatto preventiva richiesta all'Ufficio SIC il quale, successivamente, provvederà a connetterlo alla rete ed a configurarlo per l'utilizzo. Nel caso in cui l'hardware di proprietà personale non sia dotato di antivirus e che lo stesso non risulti regolarmente aggiornato, sarà negato l'accesso alla rete;
- d) NON utilizzare software di proprietà personale, anche se regolarmente acquistato e registrato a titolo personale dall'utente, ovvero software scaricato da Internet o proveniente da supporti removibili allegati a riviste e/o giornali o altro software ottenuto o posseduto a qualsiasi titolo.

5. L'Amministrazione Comunale di Tarquinia si riserva la facoltà, tramite l'Ufficio SIC della stessa e/o soggetti esterni eventualmente incaricati, di poter compiere in qualsiasi momento interventi sul sistema informativo comunale volti a garantire la sicurezza e la salvaguardia del sistema, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware etc.). Detti interventi, in considerazione dei divieti previsti dal presente regolamento, potranno anche comportare l'accesso ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica, nonché la verifica sui siti Internet a cui gli utenti abilitati alla navigazione esterna hanno avuto accesso.

6. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'Ente, si applica anche in caso di assenza prolungata od impedimento di un utente.

Art. 09 - Utilizzo dei dati e del software

1. I dati e le informazioni sono beni comunali.
2. I dati e le informazioni detenute su apparecchiature comunali o altri supporti possono essere utilizzati dall'utente autorizzato, anche fuori dagli uffici comunali, ai soli fini lavorativi.
3. Nessun dato del Comune di Tarquinia o personale degli utenti e di coloro che vengono in contatto, a qualsiasi titolo, con l'Amministrazione Comunale, detenuto per esigenze connesse al servizio, può essere trattato o memorizzato su dispositivi di qualsiasi tipologia, non finalizzati all'attività lavorativa.
4. I dati e le informazioni memorizzate, elaborate e/o comunicate attraverso le apparecchiature informatiche in uso presso il Comune di Tarquinia possono essere oggetto di controllo da parte dell'Amministrazione per esigenze legate a motivi di sicurezza o controllo di spesa od efficienza e gestione dei sistemi.
5. Sarà possibile effettuare copie di dati su supporti rimovibili solo previa autorizzazione da parte del proprio Responsabile di Settore; qualora sulle copie venissero trasferiti dati personali, gli stessi vanno utilizzati con le modalità previste dalla legge, e secondo il principio di necessità. Al termine del trattamento sarà cura dell'utente distruggere o rendere inutilizzabili i supporti rimovibili eventualmente utilizzati.
6. Si ricorda che gli applicativi gestionali (Gestione Protocollo, Atti Amministrativi, Anagrafe, ecc.) sono destinati alla gestione di informazioni il cui utilizzo deve essere compatibile con la normativa vigente relativa alla privacy (vedi d.lgs. n. 196/2003 e successive modificazioni ed integrazioni).

Art. 10 – Gestione delle credenziali d'accesso

1. Qualsiasi accesso alla rete ed agli applicativi viene associato ad una persona fisica cui collegare le attività svolte attraverso idonee credenziali di autenticazione.
2. La richiesta di rilascio delle credenziali di autenticazione deve essere trasmessa all'Ufficio SIC, via email, dal Responsabile del Settore interessato o dal Servizio Personale.
3. L'Ufficio SIC, in funzione delle esigenze operative comunicate al momento della predetta richiesta di rilascio, assegna, sospende e revoca le credenziali di autenticazione e le autorizzazioni all'accesso ai servizi hardware, software e di posta elettronica erogati dal sistema informativo attraverso le reti Intranet /Internet.
4. Le credenziali di autenticazione dell'utente sono costituite dalla coppia <User-id, Password>, vengono rilasciate secondo gli standard in uso nell'Ente e sono riconducibili alla seguente forma:
 - User-Id
 - Password alfanumerica inizializzata dall'Ufficio SIC ed obbligatoriamente cambiata al primo utilizzo da parte dell'utente.
5. Si distinguono le credenziali di autenticazione in:
 - credenziali di accesso alla rete, per l'avvio e l'utilizzo del sistema operativo e di tutte le risorse di rete;
 - credenziali di accesso ai programmi autorizzati, ciascuno con una specifica password.

6. Al primo accesso al sistema l'utente è obbligato a cambiare le password assegnate di default ed a porre in essere una gestione sicura delle stesse nel rispetto dei criteri previsti al successivo art. 11, comma 11, lett. C e D.
7. L'utente è informato del fatto che la conoscenza da parte di terzi delle credenziali, a lui riconducibili, consentirebbe a questi ultimi l'utilizzo del sistema informativo e dei servizi erogati attraverso di esso.
8. L'utente è il solo ed unico responsabile civilmente e penalmente della conservazione e della riservatezza delle proprie credenziali (d.lgs. n.196/2003 e s.m.i.) e, conseguentemente, rimane il solo ed unico responsabile per tutti gli usi ad esse connessi o correlati, (ivi compresi danni e conseguenze pregiudizievoli arrecati all'Ente e/o a terzi) siano dal medesimo utente autorizzati ovvero non autorizzati; pertanto, è impegnato a NON rivelare ad alcuno le proprie credenziali di autenticazione ed a custodirle con la massima diligenza.
9. L'utente è tenuto a comunicare quanto prima all'Ufficio SIC l'eventuale furto, smarrimento o perdita delle credenziali; in particolare, in caso di furto, l'utente si impegna a modificare tempestivamente la password utilizzando le procedure a sua disposizione.
10. Qualora sussista il dubbio di violazione della segretezza, l'utente dovrà provvedere immediatamente al cambiamento della password.
11. In caso di cessazione del rapporto di lavoro, l'account individuale dell'utente verrà dismesso secondo quanto previsto dal d.lgs. n.196/2003 e s.m.i.
12. L'utente che ottiene l'accesso alla rete ed agli applicativi si impegna ad osservare il presente regolamento e a non commettere abusi, assumendosi la totale responsabilità delle attività svolte tramite la rete di proprietà del Comune di Tarquinia.
13. Le Ditte esterne ospitate nei locali dell'Ente, così come il personale esterno incaricato dall'Ente (es. consulenti, stagisti, personale interinale) possono, previa autorizzazione, usufruire del sistema informativo comunale; l'accesso ai servizi informatici disponibili presso ciascun Settore/Ufficio deve essere attentamente valutato e chiaramente indicato nella richiesta di autorizzazione da inoltrare all'Ufficio SIC: di norma, le credenziali per il personale esterno sono a tempo e quindi, al momento del rilascio, deve essere chiaramente indicata la data di scadenza (coincidente con la fine rapporto).
14. Il personale esterno incaricato e autorizzato dall'Ente è a tutti gli effetti un utente del sistema informativo comunale ed è soggetto alle presenti norme regolamentari.
15. L'Amministratore di sistema può regolamentare l'accesso alla rete e ad Internet di determinate categorie di utenti, quando ciò sia richiesto da esigenze tecniche e di sicurezza.
16. Non è consentita l'attivazione della password di accensione (bios) del personal computer.

Art. 11 – Modalità di utilizzo degli strumenti informatici

1. Durante l'espletamento della propria attività lavorativa, i dipendenti e gli altri utenti devono attenersi alle seguenti istruzioni e raccomandazioni:

- A. ADOTTARE tutte le precauzioni e le misure di sicurezza impartite dall'Amministrazione Comunale attraverso l'Ufficio SIC, competente per la materia;
- B. EFFETTUARE una pulizia periodica (almeno una volta ogni sei mesi) dei files obsoleti e/o inutili per il prosieguo dell'attività lavorativa;
- C. UTILIZZARE password che abbiano gli adeguati standard di sicurezza determinati dall'Amministratore di sistema; a tale proposito si ricorda che, in merito alla generazione di una password, devono essere di norma seguiti i seguenti criteri e pertanto la password:
- DEVE essere diversa dallo User-ID (nome utente);
 - DEVE avere lunghezza e caratteristiche tali da non essere facilmente identificata (minimo 8 caratteri, meglio se 10 o superiori);
 - DEVE contenere almeno una lettera maiuscola, almeno una minuscola, almeno un numero e almeno un carattere speciale tra i seguenti: **! ? £ \$ % @ & # = * . +**
 - PUÒ includere caratteri dall'apparenza simili in sostituzione di altri caratteri (ad es. il numero "0" per la lettera "O" o il carattere "\$" per la lettera "S");
 - PUÒ comprendere un acronimo purché univoco e non riconducibile (ad esempio "PDRM" per "Piazza Delle Repubbliche Marinare");
 - PUÒ includere sostituzioni fonetiche o grafiche (ad esempio "6arrivato" per "Seiarrivato" o "Arrivo + tardi" per "Arrivo più tardi");
- D. EVITARE l'uso di password:
- medesime per più account;
 - utilizzate in esempi di come scegliere una buona password;
 - contenenti dati personali (nome, data di nascita, ecc.);
 - banali, ovvie, facilmente memorizzabili o riconducibili all'utente;
 - costituite da predefinite sequenze alfanumeriche;
 - contenenti parole o acronimi che si possono trovare nel dizionario;
 - contenenti sequenze di lettere/numeri sulla tastiera (asdf, 1234);
 - contenenti solo numeri, solo lettere maiuscole o solo minuscole;
 - ripetizioni di caratteri (aa11);
- E. PROCEDERE alla modifica della parola chiave al primo utilizzo e, successivamente, almeno ogni tre mesi (d.lgs 196/2003 e s.m.i.);
- F. NON è consentito modificare la configurazione impostata sul proprio PC e installare periferiche (hard-disk, DVD, fotocamere, apparati multimediali, periferiche USB, ecc.) esterne agli strumenti in dotazione se non per esigenze di servizio, autorizzate dal Responsabile di Settore di riferimento, di concerto con l'Ufficio SIC;
- G. NON è consentita la consultazione, memorizzazione e diffusione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o /o politica;
- H. NON è consentito installare, senza la necessaria autorizzazione, modem che sfruttino il sistema di comunicazione telefonica per l'accesso ad Internet o a banche dati esterne;
- I. NON è consentito agli utenti duplicare e/o cedere programmi e altro materiale informatico, se non nelle forme e per gli scopi di servizio per i quali sono stati assegnati e nel rispetto della legislazione vigente;
- J. BLOCCARE il personale computer (ad esempio, mediante l'utilizzo di CTRL+ALT+CANC # "Blocca Computer"), oppure UTILIZZARE un salvaschermo dotato di password (a tale proposito si sottolinea che lo screen saver dovrà essere consoni all'ambiente lavorativo e NON deve riprodurre immagini offensive, irrispettose o fotografie in cui siano individuabili persone, situazioni e momenti soggetti a riservatezza e/o a tutela dell'immagine di persone) ogni volta che, per qualsiasi motivo, viene lasciata incustodita la propria postazione di lavoro; in alternativa SPEGNERE fisicamente il computer;
- K. RIMUOVERE fisicamente e custodire l'eventuale hardware di autenticazione e gli altri supporti removibili ogni volta che, per qualsiasi motivo, viene lasciata incustodita la propria postazione di lavoro;

L. SPEGNERE correttamente il personal computer affidato al termine della giornata lavorativa (si ricorda che lasciare acceso inutilmente il PC, oltre a costituire un potenziale rischio elettrico ove lasciato incustodito, costituisce un inutile spreco di risorse energetiche con conseguente aggravio di costi e fonte di inquinamento ambientale).

Art. 12 - Uso di supporti removibili

1. Gli utenti che necessitano, per ragioni attinenti allo svolgimento dell'attività lavorativa, di utilizzare supporti di memorizzazione removibili (ad es. CD, DVD, cassette, cartucce, "chiavette", supporti USB e similari) devono farne richiesta al Responsabile del Settore di appartenenza ed ottenerne la preventiva autorizzazione.
2. Tutti i supporti removibili contenenti dati personali, sia comuni che sensibili, devono essere trattati con particolare cautela. In alcuni casi, infatti, è possibile recuperare i dati memorizzati anche dopo la loro cancellazione; pertanto il supporto, al termine dell'utilizzo, deve essere formattato prima di essere riutilizzato, oppure distrutto.
3. Non è consentito copiare files di provenienza incerta da supporti removibili per finalità non attinenti alla propria prestazione lavorativa onde evitare di introdurre virus nel sistema informativo comunale.
4. I supporti rimovibili contenenti dati sensibili o giudiziari, se non utilizzati, devono essere distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri dipendenti, non autorizzati al trattamento degli stessi dati, solo se le informazioni precedentemente in essi contenute sono state rese non intelligibili e non ricostruibili in alcun modo dal competente personale dell'Ufficio SIC.
5. Non è consentito l'uso di dispositivi di memorizzazione removibili scrivibili personali.
6. In caso di utilizzo di dispositivi di memorizzazione rimovibili assegnati dall'Ente, l'utente dovrà comunque provvedere alla custodia e all'uso dei medesimi adottando tutti gli accorgimenti necessari per evitare accessi non autorizzati e/o trattamenti non consentiti dei dati in essi contenuti; in particolare, dovrà distruggere i dati sul dispositivo al termine del loro utilizzo per evitare la creazione di copie non controllate.

Art. 13 - Gestione degli accessi alla rete comunale

1. Il collegamento ai servizi di rete messi a disposizione dal Comune di Tarquinia è finalizzato in via prioritaria al loro utilizzo per lo svolgimento dell'attività lavorativa.
2. La rete informatica è dotata di idonei strumenti finalizzati ad evitare che l'utilizzo dei servizi avvenga per finalità che esorbitino dalle funzioni del singolo dipendente o utente autorizzato.
3. NON è consentito accedere o collegarsi alla rete informatica comunale, con strumenti informatici non assegnati in dotazione dall'Amministrazione stessa, salvo specifica autorizzazione preventiva dell'Amministratore di sistema; l'utilizzo dei predetti strumenti deve, comunque, essere correlata a specifiche esigenze di servizio.
4. Possono accedere alla rete informatica i seguenti utenti:
 - a. gli amministratori,
 - b. il personale comunale, indipendentemente dalla natura del rapporto di lavoro;

- c. le Ditte appositamente autorizzate dall'Ufficio SIC per installare, rimuovere, mantenere programmi e software applicativi di cui siano fornitori;
- d. collaboratori esterni per il periodo in cui svolgono il proprio incarico e purché preventivamente autorizzati dall'Ufficio SIC;
- e. utenti esterni, appositamente autorizzati mediante il rilascio di specifica password che ne identifichi l'identità.

Art. 14 - Postazioni di Lavoro (PDL)

1. La configurazione base dell'hardware e l'installazione del software nelle postazioni di lavoro e negli apparati di rete di proprietà dell'Ente è effettuata dall'Ufficio SIC, quale struttura a ciò dedicata, ed è eseguita o da personale interno incaricato appartenente a detto Ufficio ovvero da personale esterno espressamente incaricato ed autorizzato.
2. L'installazione successiva di qualsiasi specie di software, dotato o meno di licenza d'uso a titolo oneroso, ovvero di periferiche deve essere effettuata solo dal personale dell'Ufficio SIC o da personale esterno incaricato.
3. Ad ogni utente può essere assegnata apposita area di lavoro dedicata e/o una cartella condivisa su server/storage di dominio per la memorizzazione di dati e programmi accessibili ad un gruppo di utenti preventivamente autorizzati.
4. L'utente è tenuto ad utilizzare le unità di rete per la condivisione di informazioni strettamente professionali; non può pertanto collocare, anche temporaneamente, in queste aree qualsiasi file che non sia attinente allo svolgimento dell'attività lavorativa.
5. Particolare attenzione deve essere prestata alla duplicazione dei dati al fine di evitare, salvo casi eccezionali, un'archiviazione superflua.
6. L'Ufficio SIC provvede al salvataggio/backup delle basi dati e dei documenti presenti sui server/storage di dominio del Comune di Tarquinia.
7. L'utente DEVE conservare tutti i dati di lavoro nelle cartelle di rete, al fine di favorire la sicurezza dei dati, con la consapevolezza che tutti i dati contenuti nel computer locale sono maggiormente soggetti a perdita in caso di guasto del sistema; il salvataggio e la salvaguardia dei dati presenti sul disco locale della postazione di lavoro sono ad ESCLUSIVA cura dell'utente.

Art. 15 - Assistenza su PDL

1. L'eventuale malfunzionamento o danneggiamento del personal computer deve essere tempestivamente comunicato all'Ufficio SIC tramite richiesta di assistenza inoltrata via e-mail.
2. Il personale incaricato ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni (PC), al fine di garantire l'assistenza tecnica e la normale attività operativa, nonché la massima sicurezza contro virus, spyware, malware, etc. e/o per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento, sostituzione, implementazione di programmi, manutenzione hardware etc.).
3. L'intervento viene effettuato esclusivamente su richiesta dell'utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica da parte dell'Ufficio SIC di problemi nel sistema informativo

e telematico; in quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, l'Ufficio SIC provvederà a dare comunicazione della necessità dell'intervento stesso.

4. L'Amministratore di sistema, i sistemisti ed i tecnici che hanno in gestione e seguono la manutenzione dei componenti del sistema informativo comunale possono procedere, dandone prima preavviso, alla rimozione dei files o applicazioni che siano ritenuti pericolosi per la sicurezza sia dai singoli personal computer, sia dalle unità di rete, procedendo comunque anche senza preavviso in casi di elevata emergenza.

Art. 16 - Utilizzo della posta elettronica

1. Il servizio di posta elettronica erogato dal sistema informativo comunale è ad uso esclusivo del Comune di Tarquinia.

2. La gestione delle caselle e-mail avviene in modo centralizzato; il servizio è erogato secondo i massimi standard di sicurezza garantendo elevata disponibilità e possibilità di essere fruito sia dalla rete comunale che dall'esterno tramite PC, smartphone, tablet etc.

3. La casella di posta elettronica assegnata nella forma `ncognome@comune.tarquinia.vt.it` (dove "n" sta per iniziale del nome) è uno strumento di lavoro; il suo utilizzo è pertanto consentito solo per finalità connesse allo svolgimento della propria attività lavorativa e per le comunicazioni di servizio di carattere istituzionale.

4. Le persone assegnatarie di un account di posta elettronica sono responsabili del corretto utilizzo dello stesso.

5. L'assegnazione dell'indirizzo di posta elettronica può avvenire contestualmente all'assegnazione delle credenziali di autenticazione dell'utente o secondo necessità.

6. L'invio e la ricezione di messaggi di posta elettronica è consentito per lo scambio di comunicazioni e documenti utili all'esercizio della propria attività lavorativa; tale modalità va utilizzata ordinariamente. Al riguardo si evidenzia che:

- a) il **"MANUALE DI GESTIONE** per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione **dei flussi documentali e degli archivi** e TITOLARIO per la classificazione dei documenti", **approvato con deliberazione di Giunta comunale n. 153 del 09-08-2016**, al Capitolo 5.3.7. RICEZIONE DI DOCUMENTI INFORMATICI SULLA CASELLA DI POSTA ELETTRONICA ORDINARIA – PEO, dispone: "Lo scambio di informazioni e comunicazioni non ufficiali, quindi solo **per le comunicazioni interne**, per le quali non occorre l'attribuzione di un numero e della data di protocollo generale **avvengono con l'utilizzo della posta elettronica ordinaria o di servizio**";
- b) l'ALLEGATO 4 - POSTA ELETTRONICA (PEO/PEC), del predetto Manuale di Gestione, delinea le **Regole Generali per l'uso della PEO** tra le quali **l'uso della stessa "[...] dai dipendenti e dall'Amministrazione per lo scambio di comunicazioni inerenti il rapporto di lavoro"**.

7. Ogni comunicazione via posta elettronica con soggetti esterni od interni all'Amministrazione deve avvenire mediante l'utilizzo del sistema di posta elettronica comunale, per garantire i necessari livelli di sicurezza e riservatezza.

8. Qualora si necessiti di attestazione ufficiale è invece necessario utilizzare la PEC tramite Protocollo Informatico. La PEC è un tipo particolare di posta elettronica, disciplinata dalla legge italiana, che permette di dare a un messaggio di posta elettronica lo stesso valore legale di una raccomandata con avviso di ricevimento tradizionale garantendo così il non ripudio.

9. Nell'utilizzo della posta elettronica aziendale l'utente è tenuto ad osservare alcune norme di comportamento, quali:

- LEGGERE quotidianamente i messaggi di posta elettronica.;
- EDITARE messaggi preferibilmente di solo testo, evitando ove possibile ogni formattazione e inserzione di immagini / motivi decorativi;
- INVIARE messaggi sintetici che descrivano in modo chiaro la questione;
- INDICARE sempre chiaramente l'oggetto, in modo tale che il destinatario possa immediatamente individuare l'argomento del messaggio ricevuto, facilitandone la successiva ricerca per parole chiave;
- MANTENERE in ordine la casella di posta elettronica cancellando mail inutili e soprattutto allegati ingombranti;
- ELIMINARE periodicamente i messaggi di posta elettronica considerati obsolete;
- RISPETTARE le regole e le indicazioni operative che verranno eventualmente fornite dall'Ufficio SIC;
- NON inviare messaggi di posta elettronica a indirizzi plurimi particolarmente numerosi se non in casi motivati da esigenze di servizio;
- NON immettere in rete informazioni che possano presentare forme o contenuti di carattere pornografico, osceno, blasfemo, razzista, diffamatorio o offensive;
- NON trasmettere dati sensibili se non precedentemente criptati;
- NON trasmettere e/o ricevere mail di carattere personale o, comunque, non attinenti ai compiti di ufficio;
- NON trasmettere e/o ricevere mail con allegati contenenti filmati o brani musicali (es.mp3) non legati all'attività lavorativa;
- NON trasmettere e/o ricevere messaggi personali o per la partecipazione a dibattiti aste on line, concorsi, forum o mailing-list;
- NON partecipare a catene telematiche (o di Sant'Antonio). Se si dovessero peraltro ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al personale dell'Ufficio SIC; NON si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi;
- NON divulgare contenuti illeciti o altrimenti inaccettabili, oppure finalizzati a violare i diritti legali altrui;
- NON violare il segreto della corrispondenza personale e il diritto alla riservatezza.

10. All'utente è vietato intercettare, alterare, impedire o interrompere comunicazioni di altri utenti ed installare apparecchiature e programmi idonei a tale scopo, salvo che queste attività non siano atte a garantire specifiche misure di sicurezza e ben determinati interventi di manutenzione e risoluzione guasti.

11. Le comunicazioni inviate e/o ricevute conterranno l'avvertimento al/ai destinatario/ri sulla natura non personale del messaggio stesso secondo le seguenti specifiche:

COMUNE DI TARQUINIA - Ufficio/Settore xxxx
Funzione per esteso (qualora fosse presente) Nome Cognome
P.zza G. Matteotti, 6 – 01016 Tarquinia (VT)
Tel. (+39) 0766 849.XXX Fax
(+39) 0766 849.270
e-mail: xxxxxxx@comune.tarquinia.vt.it

**** Riservatezza / Confidentiality ****

In ottemperanza al D.Lgs. n. 196 del 30/6/2003 in materia di protezione dei dati personali, le informazioni contenute in questo messaggio sono strettamente riservate ed esclusivamente indirizzate al destinatario indicato (oppure alla persona responsabile di rimmetterlo al destinatario). Vogliate tener presente che qualsiasi uso, riproduzione o divulgazione di questo messaggio è vietato. Nel caso in cui aveste ricevuto questo messaggio per errore, vogliate cortesemente avvertire il mittente e distruggere il presente messaggio.

According to Italian law D.Lgs. 196/2003 concerning privacy, if you are not the addressee (or responsible for delivery of the message to such person) you are hereby notified that any disclosure, reproduction, distribution or other dissemination or use of this communication is strictly prohibited. If you have received this message in error, please destroy it and notify us by email.

12. Sarà comunque consentito al superiore gerarchico dell'utente o, comunque a persona individuata dall'Ente, accedere alla casella di posta elettronica dell'Utente per ogni ipotesi in cui si renda necessario verificare la corretta rispondenza al presente regolamento, in presenza dell'utente stesso.

13. Nel caso di assenza dell'utente dal servizio dovrà essere impostata, attraverso le funzionalità del software di posta elettronica, la regola di risposta automatica che consente di inviare messaggi di risposta automatica contenenti l'indirizzo di un altro soggetto da contattare od altre utili modalità di contatto dell'unità organizzativa presso la quale l'utente opera.

14. L'assegnazione di un indirizzo di posta elettronica generico assegnato ad un Settore (ad es. nomeufficio@comune.tarquinia.vt.it) può essere richiesto esclusivamente dal Responsabile del Settore il quale fornirà indicazioni sugli utenti che dovranno essere abilitati dall'Ufficio SIC ad utilizzare tale tipologia di indirizzo.

Art. 17 - Utilizzo di Internet

1. Il collegamento ad Internet è finalizzato all'utilizzo per lo svolgimento dell'attività lavorativa.

2. Per ragioni di sicurezza e per garantire l'integrità dei sistemi informativi, l'accesso ad Internet è effettuato tramite elaboratori connessi alla rete comunale, è scrupolosamente protetto da appositi dispositivi di sicurezza informatica (firewall, antivirus, etc.) e può essere consentito per quote orarie, determinate secondo esigenze di servizio.

3. L'abilitazione per l'accesso ad Internet, o l'esclusione dall'uso di Internet, è richiesto per ciascun utente dal Responsabile del Settore competente al Responsabile del Settore da cui dipende l'Ufficio SIC.

4. Agli Utenti che si connettono ad Internet NON è consentito:

- a. l'utilizzo sistematico della rete per la visualizzazione o l'ascolto di contenuti multimediali non strettamente correlati ad esigenze di servizio ed alla specifica attività lavorativa da svolgere;
- b. registrarsi a siti, mailing-list, forum, bacheche elettroniche o altri servizi online senza specifica autorizzazione in tal senso da parte del proprio Responsabile e purché relativi a siti istituzionali ed attinenti alla propria attività lavorativa;
- c. partecipare a forum, chat line, bacheche elettroniche e social network (ad esempio Facebook e similari); l'eventuale partecipazione è permessa dall'Amministrazione in forma espressa unicamente per motivi istituzionali o professionali;

- d. il download, anche se gratuito, o la condivisione via Internet/Extranet/Intranet di file, anche di tipo audio/video o immagini, e di software non legati alle attività professionali;
- e. prelevare da Internet e/o archiviare sul proprio elaboratore, ovvero sulle risorse di rete condivise, documenti informatici (testo, audio, immagini, filmati, etc.) di natura oltraggiosa, discriminatoria per sesso, religione, origine etnica appartenenza sindacale o politica o che comunque possano risultare offensivi della dignità umana;
- f. diffondere attraverso Internet materiale commerciale o pubblicitario non richiesto;
- g. trasmettere via Internet virus, worms, trojan-horses o altro codice maligno, noto per arrecare danni e malfunzionamenti a sistemi informatici;
- h. installare o utilizzare software "peer to peer", finalizzato allo scambio e alla diffusione tramite la rete Internet, di materiale protetto dalla normativa vigente in tema di tutela del diritto d'autore;
- i. l'utilizzo di strumenti di file sharing di qualsiasi natura, esclusi quelli eventualmente resi disponibili dall'Ufficio SIC
- j. l'uso e la navigazione su siti di tipo Xrated, Casinò virtuali, Webchat basate su java, siti Warez e similari ed in particolare effettuare accessi o consultazione di materiale pornografico, pedopornografico, osceno o più in generale di qualsiasi materiale avente contenuto contrario a norme di legge, all'ordine pubblico ed al buon costume;
- k. l'uso di meccanismi o strumenti di qualsiasi natura atti ad eludere i sistemi di controllo di accesso e/o sicurezza di qualsiasi server interno o pubblico nonché gli schemi di protezione da copia abusiva del software, a rivelare password, ad identificare eventuali vulnerabilità della sicurezza dei vari sistemi, a decrittare file crittografati o a compromettere la sicurezza della rete in qualsiasi modo;
- l. fornire a soggetti non autorizzati l'accesso alla connessione Internet comunale;
- m. utilizzare la connessione Internet al fine di recare danno o disturbo a terzi;
- n. effettuare transazioni commerciali e/o finanziarie di natura personale, ivi comprese operazioni di remote banking, acquisti online e simili;
- o. modificare o mascherare le impostazioni di rete assegnate (i.e. IP address) o aggirare o disabilitare i dispositivi preposti alla gestione della sicurezza e delle comunicazioni in rete (i.e. Firewall, proxy, Router, ecc.);
- p. esprimersi in nome e per conto del Comune di Tarquinia, se non preventivamente autorizzato.

5. Il Comune di Tarquinia, si riserva la facoltà di filtrare, per il tramite dell'Amministratore di sistema, i siti, o i gruppi di siti, attivando apposite black list (siti interdetti alla navigazione dalla rete interna) e/o definendo specifici profili, o modalità particolari per tempo e orario, al fine di impedire l'accesso a siti Internet non attinenti ai compiti di ufficio ed evitare gravi minacce e problemi per la sicurezza del sistema e delle informazioni in esso contenute.

6. L'accesso alla rete Internet avviene esclusivamente attraverso apparati dedicati e dotati di appositi filtri che impediscono l'accesso a siti a carattere pornografico, di violenza, razzista, ecc. Tuttavia il sistema di filtro non garantisce l'interdizione al 100% di determinati siti; pertanto l'utente è tenuto ad attenersi a quanto già indicato.

7. Il sistema registra i dati di traffico che, su richiesta dell'autorità giudiziaria, verranno messi a disposizione per le attività di indagine.

8. E' facoltà dell'Amministrazione disporre di opportuni controlli del traffico web nel rispetto delle normative vigenti e del presente regolamento.

Art. 18 - Monitoraggio e controlli

1. L'Amministrazione si riserva la facoltà di effettuare controlli sul corretto utilizzo degli strumenti informatici e telematici nel rispetto delle normative vigenti e del presente regolamento, rivolti non ad accertare l'attività lavorativa, ma eventuali condotte illecite degli utenti.
2. L'Amministrazione, per la suddetta attività, potrà effettuare controlli a campione, sul corretto utilizzo degli strumenti informatici, della posta elettronica e di Internet avvalendosi di strumenti che consentono un controllo a distanza di tipo generalizzato, indiretto e anonimo, relativo all'intera struttura amministrativa, a singole aree, servizi o gruppi di utenti. Qualora – durante detto controllo generalizzato – vengano rilevate anomalie nell'utilizzo degli strumenti informatici, l'Amministrazione procede preliminarmente all'invio di un avviso generalizzato relativo all'uso improprio riscontrato, con l'invito ad attenersi scrupolosamente al presente regolamento e alla normativa vigente, riservandosi tuttavia la facoltà di svolgere successive azioni maggiormente mirate alla verifica del corretto utilizzo.
3. Nel pieno rispetto della normativa vigente, il Comune di Tarquinia si riserva altresì il diritto di verificare l'attuazione delle disposizioni delle presenti norme regolamentari anche attraverso l'analisi del contenuto delle informazioni tracciate dagli strumenti di monitoraggio automatici.
4. È comunque sempre fatta salva l'ipotesi dell'attivazione di controlli, anche individualizzati, che trovino giustificazione nella necessità di corrispondere ad eventuali richieste di organi di polizia su segnalazione dell'autorità giudiziaria, nel verificarsi di un evento dannoso o di una situazione di pericolo che richieda un immediato intervento o nella presenza di sospetti relativamente all'esistenza di condotte improprie nell'uso delle apparecchiature (cd. controlli difensivi).
5. In coerenza con il punto 4 della deliberazione dell'Autorità Garante per la protezione dei dati personali 1° marzo 2007, n. 13, recante "Linee guida sull'utilizzo della posta elettronica ed internet", pubblicata nella GURI n. 58 del 10 marzo 2007, non può ritenersi consentito il trattamento effettuato mediante sistemi hardware e software preordinati al controllo a distanza, grazie ai quali sia possibile ricostruire – a volte anche minuziosamente – l'attività di lavoratori. È il caso, ad esempio:
 - a) della lettura e della registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail;
 - b) della riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;
 - c) della lettura e della registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
 - d) dell'analisi occulta di computer portatili affidati in uso.

Art. 19 - Violazioni

1. Qualsiasi utilizzo del sistema informativo comunale non conforme alle disposizioni delle presenti norme regolamentari e/o alle leggi vigenti è ad esclusiva responsabilità dell'utente.
2. La violazione da parte degli utenti dei principi e delle norme contenute nel presente regolamento costituisce violazione degli obblighi e dei doveri del dipendente pubblico e, pertanto, in relazione alla gravità della violazione, il Responsabile del Settore competente, fermo restando l'obbligo di segnalazione al Segretario Generale ed alla competente Autorità Giudiziaria in caso di eventuali violazioni costituenti reato, procede all'applicazione dei necessari provvedimenti disciplinari.

Art. 20 – Norme finali

1. I dipendenti comunali dovranno attenersi, nell'utilizzo e nella gestione delle risorse informatiche strumentali, ai principi e ai doveri contenuti nel "Codice di comportamento dei dipendenti delle Pubbliche Amministrazioni" di cui al dpr n. 62/2013.
2. Il presente Regolamento costituisce parte del Regolamento di ordinamento degli Uffici e dei servizi, sostituisce pienamente il precedente ed entra in vigore con l'esecutività della deliberazione di approvazione.
3. Esso viene diffuso tra i dipendenti e tutti gli utenti che facciano utilizzo di risorse strumentali informatiche del Comune di Tarquinia perché ne prendano completa conoscenza ed adeguatamente pubblicizzato sul sito Internet dell'Ente tramite pubblicazione nella Sezione Amministrazione Trasparente.
4. Copia del presente regolamento sarà consegnata alle RR.SS.UU.
5. I Responsabili dei Settori comunali sono tenuti a vigilare affinché le presenti disposizioni siano comunicate a tutti gli utilizzatori delle risorse informatiche dell'Ente.
6. Per quanto non espressamente previsto dal presente atto, si rinvia a tutta la normativa di settore vigente.