Comune di Torri di Quartesolo
Via Roma, 174 – 36040 TORRI DI QUARTESOLO (VI)
Codice Fiscale – Partita Iva : 00530900240
Posta Elettronica Certificata (**PEC**) : torridiquartesolo.vi@cert.ip-veneto.net
Official Web Site : www.comune.torridiquartesolo.vi.it

Sistema di Qualità Certificato
UNI EN ISO 9001:2008
Certificato n. 9159.CDTQ

REGOLAMENTO PER L'UTILIZZO DELLE RISORSE INFORMATICHE DEL COMUNE DI TORRI DI QUARTESOLO

Approvato con deliberazione della Giunta Comunale n. 46 del 17-03-2016

SOMMARIO

Art. 1 – Premessa

1. Il Sistema Informativo Automatizzato, detto anche Sistema Informatico, del Comune di Torri di Quartesolo (S.I.C.) è costituito dall'insieme del patrimonio informativo digitale e delle risorse tecnologiche ed organizzative che acquisiscono, elaborano, rendono disponibile ed utilizzano tale patrimonio informativo.
2. Le risorse tecnologiche sono l'insieme degli strumenti hardware e software che permettono di accedere al patrimonio informativo digitale dell'ente, nonché alle risorse informative esterne collegate alla rete dell'ente tramite reti pubbliche o private.
3. Per Amministratore di Sistema[1] si fa riferimento al Responsabile del S.I.C. e, più in generale, di tutti i Servizi Informatici e Telematici del Comune, o suo delegato.

Art. 2 – Finalità

1. Il presente regolamento disciplina:
    a) le modalità di accesso ed utilizzo degli strumenti informatici, della rete informatica e dei servizi che tramite la stessa rete è possibile ricevere ed offrire all'interno e all'esterno dell'Amministrazione, nell'ambito dello svolgimento delle proprie mansioni ed attività di ufficio da parte degli amministratori, dipendenti e collaboratori del Comune di Torri di Quartesolo;
    b) l'individuazione del complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione per il trattamento dei dati personali, al fine di garantire l'aderenza e la rispondenza alle vigenti normative in materia, nonché adeguati livelli di sicurezza ed integrità del patrimonio informativo dell'Amministrazione Comunale.

Art. 3 – Ambito di applicazione

1. Il presente regolamento si applica a tutti gli utenti interni che sono autorizzati ad accedere alle risorse tecnologiche del sistema informatico del Comune.
2. Per utenti interni (d'ora innanzi "utenti" o "operatori") si intendono gli amministratori, i responsabili dei servizi, i dipendenti a tempo indeterminato e determinato, il personale con altre forme di rapporto contrattuale ed i collaboratori esterni impegnati in attività istituzionali, limitatamente al periodo di collaborazione.
3. Il presente regolamento è richiamato quale parte integrante nel contratto individuale di lavoro per i dipendenti o nell'atto di instaurazione della collaborazione a vario titolo con il Comune, ed è consegnato all'interessato, alla sottoscrizione del contratto stesso. Per gli utenti già in servizio al momento dell'entrata in vigore del presente Regolamento, copia del Regolamento sarà opportunamente notificato agli stessi.

[1] Con la definizione di "*amministratore di sistema*" si individuano generalmente, in ambito informatico, figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Ai fini del presente provvedimento vengono però considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi *software* complessi (art. 1 provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008, e successive modificazioni ed integrazioni).

Art. 4 – Principi generali

1. Il Comune di Torri di Quartesolo promuove l'utilizzo della Rete Informatica e Telematica, di Internet e della Posta Elettronica quali strumenti 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. I dati e le informazioni gestite ed archiviate in modalità informatica costituiscono patrimonio dell'Ente finalizzato all'erogazione di servizi istituzionali. Di conseguenza, allo scopo di consentire la piena disponibilità di tale patrimonio, la gestione informatizzata dei dati, deve privilegiare l'utilizzo di sistemi gestionali accentrati, indipendenti dalla singola postazione di lavoro, governati da livelli di autorizzazione predeterminati (user-id/password, ruolo/profilo). Pertanto, la gestione con memorizzazione delle informazioni in locale, sul proprio personal computer, deve essere ridotta al minimo e limitata ai soli casi di estrema necessità. In quest'ultima ipotesi, qualora il dipendente debba assentarsi per un periodo prolungato e programmato, deve concordare con il proprio Responsabile, le modalità per mettere a disposizione le informazioni d'ufficio memorizzate all'interno del proprio personal computer.
3. Il Comune di Torri di Quartesolo promuove, all'interno del piano annuale della formazione, anche tramite supporti documentali pubblicati nella intranet comunale, l'aggiornamento e la formazione dei propri dipendenti in merito al corretto utilizzo delle strumentazioni informatiche e telematiche.
4. Ogni utente è responsabile, civilmente e penalmente, del corretto uso delle risorse informatiche, dei servizi e dei programmi a cui ha accesso, nonché dei dati trattati a fini istituzionali.
5. Ogni utente è 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.
6. Sono vietati comportamenti che possono creare un danno, anche di immagine, all'Ente.

Art. 5 – Utilizzo del personal computer

1. Il personal computer è uno strumento di lavoro e il suo utilizzo deve essere finalizzato esclusivamente allo svolgimento delle attività professionali ed istituzionali dell'Amministrazione. Il personal computer viene assegnato all'utente in relazione alle funzioni svolte, previa autorizzazione del Responsabile del Servizio della struttura di appartenenza. Ciascuno è responsabile dell'utilizzo delle dotazioni informatiche ricevute in assegnazione. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza e, quindi, deve ritenersi vietato.
2. Il personal computer assegnato come postazione di lavoro è configurato con un profilo utente che impedisce l'installazione autonoma di nuovi programmi, per i quali deve essere fatta esplicita richiesta all'Amministratore di Sistema.
3. Ogni utente deve tenere comportamenti corretti, tali da preservare il buon funzionamento degli strumenti e tali da ridurre i rischi per la sicurezza del sistema informatico. E' vietato l'utilizzo di supporti per la memorizzazione dei dati (CD, DVD, memorie USB, etc.) non sicuri e/o provenienti dall'esterno, al fine di non diffondere eventuali virus.
4. E' necessario spegnere il personal computer al termine dell'attività lavorativa o in caso di assenza prolungata dal proprio ufficio, al fine di evitare l'accesso, anche fortuito, ai dati ivi contenuti, nonché al fine di prevenire utilizzi indebiti da parte di terzi che possono essere fonte di responsabilità. In presenza di dati personali e/o sensibili, il PC dovrà essere bloccato ogniqualvolta rimanga incustodito.

5 Non è consentita l'attivazione della password d'accensione (bios), senza preventiva autorizzazione da parte dell'Amministratore di Sistema, o suo incaricato, e, in tal caso, la suddetta password dovrà essere depositata in busta chiusa presso l'uffici dell' Amministratore di Sistema o altro locale da questi indicato.

6. I dati archiviati informaticamente devono essere esclusivamente quelli attinenti alle proprie attività lavorative.

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

8. Ogni utente deve periodicamente verificare che il programma di antivirus sia attivo e funzionante, nonché avviare un controllo antivirus per la verifica sui dischi locali del personal computer.

9. La tutela dei dati archiviati su personal computer che gestiscono localmente documenti e/o dati è demandata all'utente, il quale dovrà effettuare, con frequenza opportuna, i salvataggi su supporti dedicati ed idonei, nonché la conservazione degli stessi in luoghi adatti.

10. Non è possibile modificare le configurazioni hardware e software predefinite dagli amministratori di sistema ed installare autonomamente programmi o applicativi senza preventiva autorizzazione dell'Amministratore di Sistema.

11. E' vietata l'installazione non autorizzata di sistemi che sfruttino il sistema telefonico o reti wireless per l'accesso ad internet o ad altre reti esterne.

12. I sistemisti e i tecnici (personale interno e/o di ditte affidatarie del servizio) che hanno in gestione le componenti del sistema informatico comunale, possono, previo accordo con l'utente, procedere alla rimozione di ogni file o applicazione che riterranno essere pericolosi per la sicurezza, sia sui singoli personal computer sia sulle cartelle di rete.

13. I sistemisti e i tecnici (personale interno e/o di ditte affidatarie del servizio) incaricati della gestione e della manutenzione del sistema informatico possono, in qualsiasi momento, accedere al personal computer per attività di manutenzione preventiva e correttiva, previo accordo con l'utente. In caso di intervento manutentivo da remoto (anche con strumenti di supporto, assistenza e diagnostica remota), per il quale verrà richiesta preventivamente all'utente l'abilitazione telematica, l'utente potrà verificare le operazioni eseguite che vengono tutte visualizzate sul monitor durante la connessione.

14. Tutti i dati sensibili riprodotti su supporti magnetici devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato da terzi. Altrettanta cautela deve essere riposta in fase di stampa dei documenti contenenti dati sensibili: la stampa va effettuata su stampanti presidiate dall'addetto e, ove le attrezzature (stampanti di rete, fotocopiatrici con funzione di stampa, etc.) lo consentano, avviare la fase di stampa solo dopo aver inserito un apposito codice.

15. L'eventuale malfunzionamento o danneggiamento del personal computer deve essere tempestivamente comunicato all'Amministratore di Sistema.

16. In caso di furto è onere dell'utente, o del responsabile del servizio di appartenenza, effettuare denuncia all'autorità di polizia e far pervenire all'Amministratore di Sistema copia della denuncia.

17. Oltre a quanto sopra detto, particolare diligenza deve essere posta dall'utente di PC portatile utilizzato in ambienti esterni all'Amministrazione, sia sotto il profilo della protezione dell'apparecchiatura, sia sotto il profilo della sicurezza dei dati in essa contenuti.

18. E' responsabilità del Responsabile di ciascun Servizio compartecipare al processo di gestione della sicurezza informatica e collaborare alla verifica del coerente utilizzo delle risorse assegnate e ad evitarne sia l'uso improprio che l'accesso da parte di personale non autorizzato.

Art. 6 – Gestione utenti

1. L'abilitazione all'utilizzo delle risorse informatiche avverrà automaticamente con l'inserimento dell'anagrafica utente da parte dell'Amministratore di Sistema, su indicazione del Settore Risorse Umane. Analogamente, le variazioni di Settore o Ufficio del personale dipendente saranno automaticamente gestite dal sistema. Per gli stagisti, collaboratori esterni o altre figure simili, sarà cura di ogni Settore o dell'Ufficio Risorse Umane inoltrare richiesta all'Amministratore di Sistema, specificando gli estremi della persona interessata, nonché le date di inizio e fine dell'account richiesto.

Art. 7 – Gestione degli account e delle password

1. L'account è costituito da un codice identificativo personale (username o user-id) e da una parola chiave (password).
2. Gli account possono essere diversi, ciascuno con una specifica password, e si distinguono, in particolare:
    a) di rete, per l'avvio e l'utilizzo del sistema operativo e di tutte le risorse di rete,
    b) gestionali, per l'accesso alle applicazioni gestionali a utenti che, per motivi di servizio, ne devono fare uso.
3. La password che viene associata a ciascun utente è personale, non cedibile e non divulgabile.
4. Le password dovranno avere le caratteristiche che di volta in volta saranno segnalate dall'Amministratore di Sistema.
5. Sebbene la password sia personale e riservata, in caso di prolungata assenza ed impedimento dell'utente, che renda indispensabile ed indifferibile intervenire per esclusive necessità di operatività e sicurezza del sistema, il Responsabile del Servizio di appartenenza dell'utente, in qualità di fiduciario, potrà richiedere all'Amministratore di Sistema che venga effettuato il reset della password dell'utente medesimo. Al termine del tempo strettamente necessario al recupero delle informazioni di lavoro protette da password, il suddetto Responsabile dovrà richiedere all'Amministratore di Sistema un nuovo reset della password che, questa volta, sarà comunicato tempestivamente ed esclusivamente all'utente interessato.

Art. 8 – Utilizzo delle cartelle di rete

1. Le cartelle di rete sono aree di disco su server centrali/NAS/SAN a disposizione dei vari Settori ed Uffici. Ogni Settore avrà uno spazio la cui dimensione è limitata e determinata dall'Amministratore di Sistema, in funzione delle esigenze del settore, della disponibilità dell'intero sistema di memorizzazione, del numero di utenti, dei volumi e tipologia di documenti trattati.
2. Le cartelle di rete sono periodicamente salvate dall'Amministratore di Sistema con cadenza minima di un giorno ed i corrispondenti salvataggi sono disponibili per un arco temporale massimo di 15 giorni.
3. Le cartelle di rete sono aree di condivisione di documenti strettamente istituzionali e non possono, in alcun modo, essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia correlato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità.

4. L'organizzazione e la gestione dell'albero delle sottocartelle è demandata al Referente informatico di settore di cui al successivo art. 12. Questi ha anche il compito di effettuare una pulizia periodica degli archivi, con cancellazione dei file obsoleti, duplicati o inutili. Nel caso di un'organizzazione di settore distribuita, il referente informatico ha il compito di monitorare che la suddetta buona pratica venga messa in atto.
5. L'Amministratore di Sistema, nel caso si prefiguri un uso improprio o che metta a repentaglio la sicurezza del sistema informatico dell'Ente, ha la facoltà, previ accordi con il Referente Informatico, di procedere alla rimozione di ogni file o applicazione, nonché inibire temporaneamente l'accesso alle cartelle di rete interessate.

Art. 9 – Utilizzo delle stampanti e dei materiali di consumo

1. L'utilizzo delle stampanti e dei materiali di consumo in genere (carta, inchiostro, toner, supporti magnetici, supporti digitali) è riservato esclusivamente all'espletamento dei compiti di natura strettamente istituzionale. Devono essere evitati in ogni modo sprechi dei suddetti materiali o utilizzi eccessivi, privilegiando altresì soluzioni operative che mirino al risparmio, come ad esempio privilegiando la stampa fronte retro, nonché soluzioni operative che mirino ad evitare l'utilizzo di carta (memorizzazione di documenti scansionati e comunicazione via e-mail) nell'ottica delle direttive inerenti alla digitalizzazione della Pubblica Amministrazione.

Art. 10 – Utilizzo di Internet

1. L'utilizzo di Internet deve essere limitato a scopi inerenti l'attività lavorativa.
2. Nell'uso dei servizi Internet si devono osservare le seguenti norme comportamentali:
    - presentarsi sempre con il proprio nome, mai sotto il nome altrui;
    - non registrarsi a siti i cui contenuti non siano legati all'attività lavorativa;
    - ricordarsi che quando si scarica del materiale da Internet spesso ne viene coinvolto il diritto di proprietà intellettuale e, pertanto, è necessario ottenere esplicita autorizzazione dall'Amministratore di Sistema;
    - non trasferire sul proprio computer (download) file da siti sconosciuti e, comunque, solo per ragioni connesse all'attività lavorativa;
    - non partecipare, per motivi non professionali, a forum, chat line, ecc.;
    - non scaricare e non usare software gratuito o shareware prelevato da siti Internet, salvo i casi in cui ciò sia necessario per lo svolgimento delle proprie mansioni e previo nulla osta dall'Amministratore di Sistema;
    - nel caso di esigenza a scaricare file che richiedano la tassa di registrazione, è necessario richiedere esplicita autorizzazione scritta al proprio Responsabile.
3. L'Amministrazione, per il tramite dell'Amministratore di Sistema, adotta misure di filtraggio, che permettono di inibire o restringere l'accesso a siti i cui contenuti siano classificati pericolosi o non attinenti agli scopi istituzionali, nonché a limitare i tempi di collegamento e la banda utilizzata.
4. Sono vietate tutte le azioni atte ad eludere tali misure di filtraggio di cui al precedente comma.
5. L' Amministratore di Sistema, nel caso si prefiguri un uso improprio o che metta a repentaglio la sicurezza del sistema informatico dell'Ente, ha la facoltà di inibire temporaneamente la navigazione, anche senza preavviso, in internet alle postazioni di lavoro interessate e/o ai singoli operatori.

6. Ai soli fini di gestione e di salvaguardia giuridica degli interessi dell'Ente e dei propri dipendenti, il sistema di gestione della navigazione in internet provvede alla tracciatura secondo norma vigente, che prevede esclusivamente la registrazione delle URL senza entrare nel merito delle attività svolte (compilazione form, contenuti web-mail, etc). Il tempo di mantenimento di tali dati viene stabilito in 12 mesi, in analogia a quanto richiamato nel provvedimento del 24.07.2008 del Garante per la protezione di dati personali.

Art. 11 – Gestione e utilizzo della posta elettronica

1. Le caselle di posta elettronica rilasciate sono di due tipi:
   a) casella di posta elettronica istituzionale ordinaria – riconducibile ad un'unità organizzativa (segreteria, ragioneria, anagrafe, lavori pubblici, etc.);
   b) casella di posta elettronica individuale: casella assegnata al singolo utente.
2. Tutti i documenti e le comunicazioni inerenti i procedimenti istituzionali devono essere veicolati esclusivamente tramite gli indirizzi di posta elettronica istituzionale.
3. Le caselle di posta elettronica individuali hanno la funzione di strumenti di messaggistica (news, avvisi, passaggi informali di documenti, etc).
4. Il Responsabile del Servizio stabilisce quali utenti hanno accesso alle caselle di posta elettronica istituzionali assegnate al Settore.
5. La casella di posta elettronica assegnata è uno strumento di lavoro ed il suo utilizzo è consentito solo per finalità connesse allo svolgimento della propria attività lavorativa. Le persone assegnatarie sono responsabili del corretto utilizzo della stessa.
6. Non è consentito l'invio o la ricezione di messaggi con allegati di dimensione superiori a 15 Mb e con estensione uguali a .lnk, .bat, .exe, .scr ed in generale file di tipo eseguibile o di applicazione. Si precisa che il sistema di sicurezza e antivirus installato a protezione del server di posta elettronica del Comune di Torri di Quartesolo non consente la ricezione e l'invio di messaggi di posta che contengono allegati con le caratteristiche sopra elencate. Eventuali esigenze particolari potranno essere segnalate all'Amministratore di Sistema che individuerà la soluzione tecnica più appropriata.
7. In caso di cessazione del rapporto di lavoro o collaborazione o di mandato degli amministratori, l'indirizzo di posta elettronica individuale dell'interessato viene immediatamente rimosso, con attivazione di un messaggio automatico di ritorno che avverte che l'indirizzo e-mail non è più disponibile.
8. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e con allegati di grandi dimensioni.
9. E' vietato utilizzare l'indirizzo delle caselle di posta elettronica istituzionale e personale per l'invio o la ricezione di messaggi personali o per la partecipazione a dibattiti, forum o mailing-list, salvo diversa ed esplicita autorizzazione.
10. L'Amministratore di Sistema metterà a disposizione di tutti gli utenti apposite funzionalità di sistema che consentono di impostare un messaggio di risposta automatica (Out of Office Reply). In caso di assenza programmata, l'utente è quindi tenuto ad attivare i messaggi di risposta automatica che comunicano l'assenza dell'utente e che devono contenere i riferimenti (sia elettronici che telefonici) di Ufficio e/o utenti cui rivolgersi in caso di necessità. Nel caso, invece, di eventuale assenza improvvisa e/o prolungata (es. per malattia) e l'utente non possa attivare la procedura appena descritta, l'Amministratore di Sistema si riserva la possibilità di attivare analogo accorgimento, in accordo con il Responsabile del Servizio interessato.
11. La conservazione della posta elettronica personale è demandata ad ogni singolo utente. Nel caso in cui i messaggi o allegati debbano essere conservati, l'utente deve autonomamente

provvedere al loro salvataggio su cartelle di rete di cui all'art. 8 – "*Utilizzo delle cartelle di rete*" del presente Regolamento.

12. Ai soli fini di gestione e di salvaguardia giuridica degli interessi dell'Ente e dei propri dipendenti, il sistema di gestione della posta elettronica provvede alla tracciatura della corrispondenza in entrata e in uscita, secondo norma vigente, che prevede esclusivamente la registrazione dell'identificativo della postazione di lavoro, del mittente e del destinatario. Il tempo di mantenimento di tali dati viene stabilito in 12 mesi, in analogia a quanto richiamato nel provvedimento del 24.07.2008 del Garante per la protezione di dati personali.

Art. 12 – Referente informatico di settore

1. Ciascun Responsabile di Servizio dovrà designare per ogni settore di competenza un referente informatico. Nel caso di strutture complesse potranno essere nominati più referenti informatici in accordo con l'Amministratore di Sistema.
2. Al Referente sarà assegnato il compito di:
    a) verificare le esigenze di strumentazione informatica e segnalarle all'Amministratore di Sistema;
    b) collaborazione con l'Amministratore di Sistema nella supervisione sul corretto utilizzo delle risorse informatiche;
    c) assolvere a quanto previsto nell'art. 8 – "*Utilizzo delle cartelle di rete*" del presente Regolamento.
3. I referenti dovranno avere conoscenze idonee al ruolo.

Art. 13 – Controlli e responsabilità

1. L'Amministrazione si riserva di effettuare controlli sul corretto utilizzo degli strumenti informatici e telematici nel rispetto delle normative vigenti e del presente regolamento, nonché nel rispetto dello Statuto dei Lavoratori.
2. Per esigenze organizzative, produttive e di sicurezza, l'Amministrazione effettuerà controlli automatizzati generali con l'obiettivo di individuare potenziali rischi per la sicurezza o usi impropri del sistema informatico. L'Amministratore di Sistema ha la facoltà, nell'ambito di quanto previsto dalla normativa vigente, di effettuare eventuali ulteriori approfondimenti con gradualità, nel rispetto dei principi di pertinenza e non eccedenza, qualora i controlli automatici riscontrino potenziali rischi o problemi. I suddetti procedimenti di controllo saranno opportunamente documentati (tipo di controlli, nome del sistemista che opera i controlli, log di accesso ai sistemi, riscontri dei controlli).
3. Qualora la tipologia dei controlli automatizzati adottati contempli la possibilità di controllo dell'attività dei lavoratori, l'attivazione sarà preceduta da un accordo con le rappresentanze sindacali aziendali, le quali inoltre saranno informate delle iniziative adottate in sede di prima applicazione del presente Regolamento.
4. Il mancato rispetto o la violazione delle norme contenute nel presente regolamento è perseguibile con provvedimenti disciplinari, nonché con le azioni civili e penali consentite.

Art. 14 – Norma di rinvio

1. Per quanto non espressamente previsto nel presente regolamento, si rinvia alle specifiche diposizioni e direttive in materia ed in particolare:

   a) Direttiva n. 2/2009 della Presidenza del Consiglio dei Ministri – Dipartimento della Funzione Pubblica "*Utilizzo di internet e della casella di posta elettronica istituzionale sul luogo di lavoro*";

   b) Delibera n. 13/2007 del Garante per la protezione dei dati personali "*Lavoro: le linee guida del Garante per la posta elettronica e internet*";

   c) Codice di comportamento dei dipendenti delle pubbliche amministrazione – Allegato al C.C.N.L. 22.01.2004.

   che, ad ogni buon fine, si allegano in copia al presente regolamento.

****