Comune di Foggia

REGOLAMENTO PER L'UTILIZZO DEL SISTEMA INFORMATICO DELL'ENTE

(Delib. G.C. del 09-02-2009 n. 32)

art. 1
Oggetto, ambito di applicazione, riferimenti normativi

1. Il presente regolamento costituisce atto normativo a valenza organizzativa, complementare al regolamento sull'ordinamento degli Uffici e dei Servizi, attuativo di quanto previsto dal regolamento comunale per il trattamento dei dati personali.
2. Il presente regolamento disciplina l'utilizzo degli strumenti informatici del Comune di Foggia, con particolare riferimento alle modalità di accesso e di uso della rete informatica e telematica e dei servizi che dalla stessa è possibile ricevere o offrire.
3. Il presente regolamento fa riferimento in particolare alle seguenti disposizioni di legge: artt 76,87,117 della Costituzione, L. 7 agosto 1990, n. 241, Direttiva 1999/93 CE, DPR 28 dicembre 2000, n. 445, ; D. Lgs 30 giugno 2003, n. 196, L. 9 gennaio 2004, n. 4, Deliberazione CNIPA 19 febbraio 2004, n. 11; L. 15 del 2005, D. Lgs 7 marzo 2005, n. 82 (Codice dell'Amministrazione digitale) e successive modificazioni ed integrazioni.

art. 2
Utilizzo del Personal Computer

1. Il Personal Computer affidato al dipendente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.
2. L'accesso all'elaboratore è protetto da password che deve essere custodita dall'incaricato con la massima diligenza e non divulgata. La stessa password deve essere attivata per l'accesso alla rete, per l'accesso a qualsiasi applicazione, per lo screen saver e per il collegamento a Internet. Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte dell'Amministratore del Sistema,
3. Non è consentito installare autonomamente programmi provenienti dall'esterno salvo previa autorizzazione esplicita dell'Amministratore del Sistema, perché sussiste il grave pericolo di portare Virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore.
4. Non è consentito l'uso di programmi diversi da quelli distribuiti ufficialmente dalla nostra amministrazione (dlg. 518/92 sulla tutela giuridica del software e L. 248/2000 nuove norme di tutela del diritto d'autore);
5. Non è consentito all'utente modificare le caratteristiche impostate sul proprio PC, salvo previa autorizzazione esplicita dell'Amministratore del Sistema.

6. Il Personal Computer deve essere spento prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. In ogni caso lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.
7. Si devono mettere in atto accorgimenti tali per cui il computer non resti, durante una sessione di trattamento:
   a) incustodito: può essere sufficiente che un collega rimanga nella stanza, durante l'assenza di chi sta lavorando con lo strumento elettronico, anche se la stanza rimane aperta
   b) accessibile: può essere sufficiente attivare lo screen saver con password oppure chiudere a chiave la stanza, dove è situato lo strumento elettronico, durante l'assenza, anche se nella stessa non rimane nessuno.
8. Non è consentita l'installazione sul proprio PC di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, switch, ecc.), se non con l'autorizzazione espressa dell'Amministratore del Sistema.
9. Agli utenti incaricati del trattamento dei dati sensibili è fatto divieto l'accesso contemporaneo con lo stesso account da più PC.
10. Ogni incaricato deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente l'Amministratore del Sistema nel caso in cui siano rilevati virus ed adottando quanto previsto dal successivo articolo 8 del presente Regolamento relativo alle procedure di protezione antivirus.
11. Non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.
12. I PC portatili utilizzati all'esterno (convegni, visite in azienda), in caso di allontanamento, devono essere custoditi in un luogo protetto.

art. 3
Utilizzo della rete

1. Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità, vengono svolte regolari attività di controllo, amministrazione e backup da parte dell'Amministratore del Sistema.
2. Le password d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite. E' assolutamente proibito entrare nella rete e nei programmi con altri nomi utente.
3. L'Amministratore del Sistema può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza sia sui PC degli incaricati sia sulle unità di rete.
4. Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. E' infatti assolutamente da evitare un'archiviazione ridondante.
5. E' cura dell'incaricato effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni. E' buona regola evitare di stampare documenti o file non adatti (molto lunghi o non supportati, come ad esempio il formato pdf o file di contenuto grafico) su stampanti comuni. In caso di necessità la stampa in corso può essere cancellata.

6. Ogni apparecchiatura collegata alla rete aziendale senza la preventiva autorizzazione dell'Amministratore del Sistema sarà ritenuta compromettente e dannosa per la qualità del servizio, anche se correttamente applicata, spetterà all'Ufficio responsabile valutarne l'opportunità.

art. 4
Gestione delle Password e delle User-id

1. Le password di ingresso alla rete, di accesso ai programmi e dello screen saver, sono attribuite dall'Amministratore del Sistema.
2. L'incaricato deve provvedere a modificare la password immediatamente, non appena la riceve per la prima volta, da chi amministra il sistema.
3. La password deve essere composta da otto caratteri e formate da lettere (maiuscole o minuscole) e numeri, ricordando che lettere maiuscole e minuscole hanno significati diversi per il sistema.
4. La password deve essere segreta e quindi non conoscibile da terzi. Ogni incaricato dovrà adottare le necessarie cautele per assicurare la sua segretezza. Ad esempio, la password non potrà essere trascritta su post-it da applicare sui monitor dei PC, né riportata sulle prime pagine della propria agenda.
5. La password non deve contenere riferimenti agevolmente riconducibili all'interessato (non solo nomi, cognomi, soprannomi, ma neppure date di nascita proprie, dei figli o degli amici)
6. La password utilizzata dagli incaricati al trattamento ha una durata massima di tre mesi, trascorsi i quali deve essere sostituita
7. Nel caso di trattamento di dati sensibili, la password utilizzata dagli incaricati al trattamento ha una durata massima di tre mesi, trascorsi i quali deve essere sostituita
8. Nessuno, neppure il Titolare del trattamento, può accedere allo strumento elettronico, utilizzando la credenziale di autenticazione dell'incaricato. Eccezione a tale regola si ha solo se verificano congiuntamente le seguenti condizioni:
   a) prolungata assenza o impedimento dell'incaricato
   b) l'intervento è indispensabile e indifferibile
   c) . vi sono concrete necessità, di operatività e di sicurezza del sistema.

   A tale fine, agli incaricati dovranno:
   a) predisporre una copia della parola chiave, provvedendo quindi a trascriverla su un foglio, facendo però in modo che l'informazione resti segreta, ed inserendola in una busta chiusa
   b) consegnino tale copia al Custode delle Password, che sia stato previamente incaricato della sua custodia;
      Solo al verificarsi delle condizioni sopra esposte, il titolare o un responsabile potranno richiedere la busta che la contiene, al Custode delle Password.

   Rientrano tra i compiti del Custode:
   a) conservare in luogo sicuro e chiuso a chiave le buste contenenti le password
   b) . provvedere ad informare, tempestivamente e per iscritto, l'incaricato cui appartiene la parola chiave, dell'accesso effettuato.
   c). verificare la regolare consegna nei tempi previsti (sei o tre mesi) delle buste con le nuove password da parte degli incaricati
9. La password deve essere immediatamente sostituita, dandone comunicazione al Custode delle Password, nel caso si sospetti che la stessa abbia perso la segretezza.

10. Qualora l'incaricato venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia alla Direzione o persona dalla stessa incaricata.
11. Il codice per l'identificazione (user-id), che l'Amministratore del Sistema provvede a fornire all'incaricato, quale componente della chiave per accedere all'elaboratore e successivamente a gestire, deve essere univoco:
    a) esso non può essere assegnato ad altri incaricati, neppure in tempi diversi.
12. Le credenziali di autenticazione (password e user-id) devono essere disattivate nei seguenti casi:
    a) immediatamente, nel caso in cui l'incaricato perda la qualità che gli consentiva di accedere allo strumento; ciò non accade solo se la persona cessa di lavorare, ma può ad esempio avvenire anche se l'incaricato viene trasferito da un ufficio all'altro, con conseguente cambio delle mansioni e degli ambiti di trattamento dei dati personali, che rendesse necessaria l'attribuzione di una nuova chiave
    b) in ogni caso, entro sei mesi di mancato utilizzo; fa ovviamente eccezione il caso delle chiavi che sono state preventivamente autorizzate per soli scopi di gestione tecnica, il cui utilizzo assume generalmente caratteristiche di sporadicità (ad esempio, potrebbero essere utilizzate solo una volta l'anno, nel quadro della verifica globale, sulla funzionalità complessiva del sistema).

art. 5
Utilizzo dei supporti magnetici

1. Tutti i supporti magnetici riutilizzabili (dischetti, cassette, CD, cartucce) contenenti dati sensibili devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato. Una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione.
2. I supporti magnetici riutilizzabili (dischetti, cassette, CD, cartucce) contenenti dati sensibili devono essere custoditi ed utilizzati in modo tale da impedire accessi non autorizzati (furti inclusi) e trattamenti non consentiti.
3. Una volta cessate le ragioni per la conservazione dei dati, i supporti non possono venire abbandonati, ma si devono porre in essere gli opportuni accorgimenti, finalizzati a rendere inintelligibili e non ricostruibili tecnicamente i dati in essi contenuti, al fine di impedire che essi vengano carpiti da persone non autorizzate al trattamento. Si devono quindi cancellare i dati, se possibile, o arrivare addirittura a distruggere il supporto, se necessario.
4. I supporti magnetici contenenti dati sensibili devono essere custoditi in archivi chiusi a chiave.
5. Non è consentito scaricare files contenuti in supporti magneto/ottici non aventi alcuna attinenza con la propria prestazione lavorativa.
6. Tutti i file di provenienza incerta od esterna, ancorché attinenti all'attività lavorativa, devono essere sottoposti al controllo ed alla relativa autorizzazione all'utilizzo.
7. Ogni incaricato deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente l'Amministratore di Sistema nel caso in cui siano rilevati virus ed adottando quanto previsto dal presente Regolamento relativo alle procedure di protezione antivirus.
8. Nel caso di utilizzo P.C. portatili accessibili per mezzo di smart card o tessere magnetiche in possesso a proprio uso esclusivo, ogni incaricato dovrà conservare (es. non abbandonandole sulla scrivania) e proteggere (es. non avvicinarle a fonti di calore) tali dispositivi con la massima cura. Per tutelarsi in

caso di furto, è altresì necessario, per l'accensione del relativo strumento elettronico, associare a tali dispositivi una password.

art. 6
Utilizzo di PC portatili

1. L'incaricato è responsabile del PC portatile assegnatogli dall'Amministratore del Sistema e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
2. Ai PC portatili si applicano le regole di utilizzo previste per i PC connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.
3. I PC portatili utilizzati all'esterno (convegni, visite in azienda), in caso di allontanamento, devono essere custoditi in un luogo protetto.

art. 7
Salvataggio e ripristino dei dati

1. I dati personali devono essere salvati con cadenza settimanale. Ogni incaricato è tenuto a controllare il regolare funzionamento dei back up, anche se fatto a livello di server, e verificare il salvataggio di tutti i files presenti nel proprio P.C..
2. Per i dati sensibili l'incaricato deve essere in grado di provvedere al ripristino dei dati entro sette giorni.

art. 8
Uso della posta elettronica

1. La casella di posta, assegnata dall'Amministrazione all'incaricato, è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
2. E' fatto divieto di utilizzare le caselle di posta elettronica aziendale nome.cognome@comune.foggia.it per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list salvo diversa ed esplicita autorizzazione.
3. E' buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.
4. Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per l'Amministrazione Comunale, ovvero contenga documenti da considerarsi riservati in quanto contraddistinti dalla dicitura "strettamente riservati" o da analoga dicitura, deve essere visionata od autorizzata. In ogni modo, è opportuno fare riferimento alle procedure in essere per la corrispondenza ordinaria.
5. E' possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario, ma di norma per la comunicazione ufficiale è obbligatorio avvalersi degli strumenti tradizionali (fax, posta, …).
6. Per la trasmissione di file all'interno è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati.
7. E' obbligatorio controllare i file attachements di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).
8. E' vietato inviare catene telematiche (o di Sant'Antonio); se si dovessero ricevere messaggi di tale tipo, si deve comunicarlo immediatamente all'Amministratore del Sistema. Non si deve in alcun caso attivare gli allegati di tali messaggi.

9. I messaggi di posta elettronica inviati e ricevuti utilizzando l'indirizzo e-mail fornito dall'Amministrazione Comunale possono essere letti, ed eventualmente stampati, da altri soggetti appartenenti all'organizzazione, purché autorizzati.

art. 9
Uso della rete Internet e dei relativi servizi

1. Il PC abilitato alla navigazione in Internet costituisce uno strumento necessario allo svolgimento della propria attività lavorativa. E' assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa. Sono pertanto vietati:
   a) l'uso di Internet per lo scarico di file del tipo MP3, AVI, MPG, Quicktime, e/o altri tipi di files o programmi freeware/shareware non legati ad un uso d'ufficio, se non espressamente autorizzato dal Responsabile del Servizio Sistemi Informativi;
   b) l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dall'Amministrazione o attinenti i compiti e le mansioni assegnate e con il rispetto delle normali procedure di acquisto;
   c) la registrazione, l'uso e la navigazione su siti non legati ad esigenze esclusivamente di tipo lavorativo, a tal fine l'Amministrazione provvederà ad inibire la consultazione dei siti web non utili alla produttività dell'Ente e, soprattutto, potenzialmente lesivi per l'infrastruttura;
   d) la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames), se non attinenti l'attività lavorativa svolta;
   e) la navigazione in siti ove sia possibile rivelare le opinioni politiche, religiose o sindacali dell'utilizzatore; non è consentito inoltre visitare siti e memorizzare documenti informatici dai contenuti di natura oltraggiosa e/o discriminatoria per sesso/etnia/religione/opinione e/o appartenenza sindacale e/o politica;
   f) l'accesso alla rete internet in orari differenti da quello di lavoro; a tal fine il responsabile della sicurezza informatica, d'accordo con i responsabili di servizio, indicherà un orario di massima per la concessione del servizio di accesso ad internet; il Servizio Sistemi Informativi si riserva di applicare per singoli e gruppi di utenti politiche di navigazione personalizzate in base alle mansioni ed eventuali disposizioni concordate con l'Amministrazione e con i Dirigenti, al fine di ottimizzare l'uso delle risorse, gli investimenti e le prestazioni delle connessioni esistenti;
   g) l'utilizzo di qualsiasi mezzo alternativo (modem o altro) al collegamento Lan dell'Ente per connettersi ad Internet;
   h) l'accesso alla rete dall'esterno via modem o con qualsiasi altro mezzo di accesso remoto senza l'autorizzazione del responsabile della sicurezza informatica;
   i) lo svolgimento di qualsiasi attività intesa ad eludere o ingannare i sistemi di controllo di accesso e/o sicurezza di qualsiasi server interno o pubblico, incluso il possesso o l'uso di strumenti o software intesi ad eludere schemi di protezione da copia abusiva del software, rivelare password, identificare eventuali vulnerabilità della sicurezza dei vari sistemi, decrittare file crittografati o compromettere la sicurezza della rete e internet in qualsiasi modo.

art. 10
Protezione antivirus

1. Ogni incaricato deve tenere comportamenti tali da proteggere i dati personali contro il rischio di intrusione e dall'azione di programmi di cui all'art. 615-quinquies del codice penale, aventi per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione totale o parziale, o l'alterazione del suo funzionamento
2. Ogni incaricato è tenuto a controllare il regolare funzionamento e l'aggiornamento periodico del software installato, secondo le procedure previste.
3. Nel caso che il software antivirus rilevi la presenza di un virus, l'incaricato dovrà immediatamente:
   a) sospendere ogni elaborazione in corso senza spegnere il computer;
   b) segnalare l'accaduto all'amministratore di sistema.
4. Non è consentito l'utilizzo di floppy disk, cd rom, cd riscrivibili, nastri magnetici di provenienza ignota.
5. Ogni dispositivo magnetico di provenienza esterna dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere consegnato all'amministratore di sistema.

art. 11
Utilizzo di supporti cartacei

1. Gli incaricati del trattamento devono prelevare dagli archivi i soli atti e documenti loro affidati, che devono controllare e custodire, durante l'intero ciclo necessario per lo svolgimento delle operazioni di trattamento, per poi restituirli all'archivio, al termine di tale ciclo.
2. Per gli atti ed i documenti contenenti dati sensibili, il controllo e la custodia devono avvenire in modo tale che ai dati non accedano persone prive di autorizzazione.
3. Per i documenti contenenti dati sensibili, è necessario che l'incaricato del trattamento utilizzi cassetti con serratura, o di altri accorgimenti aventi funzione equivalente, nei quali riporli prima di assentarsi dal posto di lavoro, anche se temporaneamente. In tali cassetti i documenti potranno essere riposti al termine della giornata di lavoro, qualora l'incaricato debba utilizzarli anche nei giorni successivi; al termine del trattamento l'incaricato dovrà invece restituirli all'archivio.
4. Agli archivi contenenti dati sensibili possono accedere sempre e comunque i soli soggetti autorizzati
5. Per gli accessi agli archivi contenenti dati sensibili che avvengono dopo l'orario di chiusura, è obbligatorio identificare e registrare coloro che vi accedono.

art. 12
Flusso documentale

1. L'informatizzazione del Comune di Foggia è estesa al trattamento dei documenti nell'ambito dei processi. Gli uffici sono tenuti ad utilizzare le applicazioni informatiche predisposte all'iter documentale e all'interoperabilità tra i Servizi.
2. Oltre a gestire l'iter dei documenti, il sistema gestisce e controlla le attività del procedimento, non è consentito pertanto utilizzare software, se pur funzionali, isolati dal sistema applicativo integrato.

art. 13
Non osservanza della normativa comunale

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

art. 14
Aggiornamento e revisione

1. Tutti gli incaricati possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Le proposte verranno esaminate dal Servizio competente.
2. Il presente Regolamento è soggetto a revisione con frequenza annuale.

art. 15
Sanzioni

1. In caso di abuso, a seconda della gravità del medesimo, e fatte salve ulteriori conseguenze di natura penale, civile e amministrativa, possono essere comminate le sanzioni disciplinari previste dalla normativa vigente in materia e dai contratti di lavoro.