COMUNE DI AFRAGOLA

PROVINCIA DI NAPOLI

REGOLAMENTO INTERNO PER L'ACQUISTO E L'UTILIZZO DEGLI STRUMENTI INFORMATICI

Adottato con deliberazione della Commissione Straordinaria
n. 204 del 18.12.07

+

Art. 1 Oggetto del Regolamento

Il presente Regolamento disciplina l'acquisto e l'utilizzo delle risorse informatiche e telematiche dell'Ente nell'intento di:

- garantire la massima efficienza delle risorse informatiche e del loro utilizzo;
- garantire la riservatezza delle informazioni e dei dati;
- provvedere ad un servizio continuativo nell'interesse dell'Ente;
- garantire il rispetto delle leggi in materia di utilizzo delle risorse informatiche;

Art. 2 Regole per l'utilizzo degli strumenti informatici

2.1 Utilizzo dei personal computer

a) Definizione: Il personal computer (postazione di lavoro) è costituito dall'elaboratore elettronico (monitor, stampanti, scanner, gruppi di continuità ecc) e dal relativo sistema operativo installato.

b) Il personal computer (PC) 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.

c) L'accesso all'elaboratore è protetto da credenziali di autenticazione conformi alla normativa in vigore (D.Lgs. 196/03). La componente riservata (parola chiave/password) deve essere custodita dall'incaricato con la massima diligenza e non divulgata. La parola chiave consente l'accesso alla rete, l'accesso alle applicazioni software. Non è consentita l'attivazione della password di accensione (bios).

d) L'Amministratore di Sistema per l'espletamento delle sue funzioni, ha la facoltà in qualunque momento di accedere ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica interna ed esterna.

e) Non è consentito installare autonomamente programmi provenienti dall'esterno salvo previa autorizzazione esplicita del dirigente di settore previa consultazione dell'Amministratore di sistema, perché sussiste il grave pericolo di portare virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore.

f) Non è consentito l'installazione e l'uso di programmi di condivisione e scambio di file tra utenti delle rete Internet (peer to peer,….). Inoltre non è consentito installare strumenti software atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o strumenti informatici.

g) Non è consentito l'uso di programmi diversi da quelli distribuiti ufficialmente dall'Ente (d.lgs. 518/92 sulla tutela giuridica del software e L. 248/2000 nuove norme di tutela del diritto d'autore).

h) Non è consentito all'utente modificare le caratteristiche impostate sul proprio PC, salvo previa autorizzazione esplicita dell'Amministratore di sistema

i) Il personal computer deve essere spento ogni sera 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. In ogni caso deve essere attivato lo screen saver e la relativa password.

j) Non è consentita l'installazione sul proprio PC di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, ….) , se non con l'autorizzazione espressa dell'Amministratore di Sistema.

k) Agli utenti incaricati del trattamento di dati è fatto divieto l'accesso contemporaneo con lo stesso account da più elaboratori per lo stesso applicativo software.

l) Ogni utente 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 successivo punto 8.8 del presente Regolamento relativo alle procedure di protezione antivirus.

m) 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.

n) Devono essere prontamente segnalati, per iscritto all'Amministratore di Sistema:
   1) Il furto
   2) Il danneggiamento o lo smarrimento degli strumenti informatici
   3) Ogni malfunzionamento hardware e software (nel caso che il servizio di manutenzione sia esternalizzato vanno utilizzati i moduli predisposti dall'azienda affidataria del servizio).

   Tali segnalazioni sono necessarie per poter ottenere una dichiarazione dell'Amministratore di Sistema sull'intervento più efficiente e conveniente per l'Ente.

o) L'Amministrazione ha la facoltà di aggiornare le dotazioni hardware e software ivi installato presso ciascun utente con altre, anche precedentemente utilizzate all'interno dell'Ente, con lo scopo di incrementare globalmente le prestazioni e l'operatività di ciascun elaboratore elettronico. Le prestazioni dell'elaboratore elettronico sono dimensionate sulla base delle applicazioni software utilizzate.

p) E' consentito l'uso di tecniche di cifratura dei dati trattati, solo se necessario, ed esclusivamente mediante software distribuiti dall'Ente. Copia della chiave di decodifica (chiave privata,….) deve essere consegnata, in busta chiusa, al dirigente (o altro custode della password designato) in base alla modalità descritte nelle istruzioni operative.

2.2 Uso della rete Comunale (Intranet)

a) 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 di sistema e dagli incaricati individuati da quest'ultimo.

b) Le password d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo procedure impartite. E' assolutamente proibito entrare nella rete e nei programmi con altri nomi utente.

c) Per garantire la manutenzione della sicurezza e della rete, soggetti autorizzati dall'Amministrazione (di norma Amministratori di sistema e aziende esterne autorizzate) possono monitorare gli apparati, i sistemi ed il traffico in rete in ogni momento.

d) 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.

e) E' cura dell'utente 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.

f) L'amministratore di sistema può in qualunque momento procedere alla rimozione o disattivazione di ogni file e applicazione che riterrà essere pericolosi per la sicurezza ed integrità dei dati sia sui singoli personal computer degli incaricati sia sulle unità di rete.

g) Qualora si verifichino situazioni di grave minaccia della sicurezza e integrità del sistema informatico aziendale un elaboratore elettronico potrà, anche senza preavviso , essere sospeso dal collegamento alla rete comunale fino al ripristino delle condizioni tecniche che garantiscono la sicurezza della connessione stessa.

h) Non è consentito collegare sistemi informatici di soggetti terzi esterni se non con l'autorizzazione espressa dell'Amministratore di sistema. Assicurarsi che i sistemi di soggetti terzi, esterni, qualora interagiscano con il sistema informatico dell'Amministrazione, siano dotati di adeguate misure di protezione antivirus.

2.3 Utilizzo delle credenziali di autenticazione e gestione delle password (parola chiave)

a) Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione (identificativo e password) necessarie per accedere alle risorse informatiche e alle applicazioni software; l'incaricato deve adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo.

b) Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.

c) Le credenziali di autenticazione devono essere disattivate:
   1) se non utilizzate da almeno sei mesi, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica;
   2) in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

d) Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante l'uso della componente riservata della credenziale per l'autenticazione (parola chiave/password), sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso, la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia (*custode delle parole chiave*), i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.

e) Il custode delle parole chiave (password) se non è nominato specificatamente coincide con il proprio dirigente di settore o responsabile dell'ufficio/servizio.

f) La comunicazione al custode delle parole chiave avviene secondo le seguenti modalità:
   1) Per iscritto su carta in cui riportare: data, nome e cognome dell'utente, l'elaboratore (n. catalogo riportato sulla nota di assegnazione) oppure l'applicativo al quale consentono l'accesso e/o il file o la cartella che proteggono;
   2) Chiuse in busta.

g) Le password (parola chiave) sono inizialmente attribuite dall'Amministratore di sistema. Deve essere successivamente effettuata l'autonoma modifica da parte degli incaricati al trattamento e, se necessario, contestuale comunicazione al custode delle parole chiavi.

h) La password, quando è prevista dal sistema di autenticazione, è composta da almeno 8 caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.

i) La password deve essere immediatamente sostituita, dandone comunicazione al custode delle parole chiave, nel caso si sospetti che la stessa abbia perso la segretezza.

j) L'utente è ritenuto responsabile, sin dal momento della assegnazione, delle attività e delle sessioni di trattamento dati effettuate sull'elaboratore elettronico con le credenziali assegnate.

2.4 Utilizzo dei supporti magnetici

a) I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcuni modo ricostruibili

b) I supporti magnetici contenenti dati sensibili devono essere custoditi in archivi controllati (chiusi a chiave, …..).

c) Non è consentito scaricare files contenuti in supporti magnetici/ ottici non aventi alcuna attinenza con la propria prestazione lavorativa.

2.5 Utilizzo di personal computer portatili

a) L'utente è responsabile del PC portatile assegnatogli dall'Amministratore di sistema e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

b) 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.

2.6 Uso della rete Internet e dei relativi servizi

a) Il PC abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario per lo svolgimento della propria attività lavorativa. E' assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.

b) E' fatto divieto all'utente lo scarico di software gratuito (freeware) e shereware prelevato da siti Internet, se non espressamente autorizzato dall'Amministratore di sistema.

c) E' tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti online e simili salvo i casi direttamente autorizzati e con il rispetto delle normali procedure di acquisto.

d) E' da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.

e) E' vietata 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).

f) Sono vietati i collegamenti diretti dei PC alle linee telefoniche convenzionali attraverso modem. I collegamenti attraverso le linee telefoniche convenzionali (analogiche e digitali) rappresentano una significativa minaccia per l'Ente di attacchi esterni. L'eventuale installazione ed utilizzo di modem deve essere autorizzata dall'Amministratore di sistema.

g) Non sono ammessi cellulari per realizzare collegamenti dati facilmente intercettabili o che consentono un reistradamento della connessione.

h) Gli elaboratori potranno essere abilitati all'uso della rete Internet, compatibilmente con le esigenze di bilancio, a seguito di autorizzazione scritta del dirigente responsabile del servizio o dell'area previa consultazione dell'Amministratore di sistema riguardo alla compatibilità del sistema operativo e software, installati sull'elaboratore oggetto della richiesta e ai requisiti di sicurezza.

i) Al solo scopo di documentare eventuali comportamenti illeciti e per esigenze statistiche e di controllo della spesa, questa Amministrazione ha attivato sistemi software in grado di monitorare, per ogni postazione, i siti a cui si effettua la connessione.

2.7 Uso della posta elettronica

a) La casella di posta è uno strumento di lavoro, concessa in uso al singolo utente per lo svolgimento dell'attività amministrativa ad esso demandata, la cui titolarità, pertanto è inequivocabilmente riconducibile all'Amministrazione stessa. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

b) E' fatto divieto di utilizzare le caselle di posta elettronica dell'Ente, per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list salvo diversa esplicita autorizzazione.

c) La posta elettronica resta comunque un bene aziendale, come tale accessibile ai soggetti autorizzati e al datore di lavoro.

d) Non esiste un diritto all'utilizzo esclusivo da parte dell'utente di una casella di posta elettronica, pertanto in caso di necessità l'Amministrazione si riserva il diritto, in qualità di proprietario del bene, di accedere al contenuto della casella di posta, di ☐assegnare l'uso della casella di posta ad altro utente, di effettuare controlli sull'uso.

e) E' buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi. La casella di posta elettronica deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

f) Non è consentito l'utilizzo dell'indirizzo di posta elettronica aziendale per la partecipazione a dibattiti, forum o mail-list, salvo diversa ed esplicita autorizzazione.

g) Per la trasmissione di file all'interno dell'Ente, è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati.

h) E' obbligatorio controllare i file allegati (attachements) di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o ftp non conosciuti).

i) E' vietato utilizzare catene telematiche (o di Sant'Antonio). Non si deve in nessun caso attivare gli allegati di tali messaggi.

2.8 Protezione antivirus

a) Tutti i PC, i server ed i sistemi di elaborazione in genere, che sono connessi in rete interna dell'Amministrazione (intranet) e/o esterna (internet/extranet) di proprietà dell'Amministrazione o del personale, devono essere dotati di un sistema antivirus approvato dall'Amministratore di sistema (o responsabile della sicurezza) ed aggiornato.

b) Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico comunale mediante virus o mediante ogni altro software aggressivo.

c) Ogni utente è tenuto a verificare il regolare funzionamento e l'aggiornamento periodico del software installato, secondo le procedure previste e non può in nessun caso disattivarlo.

d) Nel caso che il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente:
   1) sospendere ogni elaborazione in corso senza spegnere il computer;
   2) segnalare l'accaduto all'Amministratore di sistema.

e) Non è consentito l'utilizzo di floppy disk, cd rom, cd riscrivibili, nastri magnetici di provenienza ignota.

f) Ogni dispositivo magnetico, ottico ed elettronico di provenienza esterna all'Ente 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. 3 Regole per l'acquisto della strumentazione informatica (Hardware e Software)

L'acquisto di strumentazione hardware e software deve essere sottoposta alla valutazione tecnica del Responsabile dei Servizi Informatici.

Tale obbligo si rende necessario per ragioni di sicurezza, efficienza ed omogeneità del Sistema Informativo Comunale.

3.1 Acquisto di strumentazione hardware e software

a) L'acquisto di strumentazione hardware (stampanti, personal computer, server, etc.) e software (applicativi per l'automazione d'ufficio, applicativi di supporto alle attività dell'Ente, etc.), da parte dei Settori dell'Ente, deve essere preceduta da una richiesta di relazione tecnico/funzionale attestante la compatibilità con il Sistema Informativo Comunale, indirizzata al Responsabile dei Servizi Informatici. Tale richiesta deve essere accompagnata da tutte le informazioni tecniche necessarie per una corretta valutazione.

b) Il Responsabile dei Servizi Informatici deve produrre una relazione tecnica entro 7gg. lavorativi dal ricevimento della richiesta indicata nell' art. 3.1 lettera a.

c) Visto il regolamento di contabilità (art. da 54 a 62) si rende obbligatorio l'iscrizione, nel patrimonio dell'Ente(inventario dei beni mobili), di ogni acquisto, noleggio, cessione, distribuzione o donazione di strumentazione informatica.

Art. 4 Norme conclusive

4.1 Non osservanza del regolamento

a) 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.

4.2 Aggiornamento e revisione

a) Tutti i Dirigenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento.

b) Il presente Regolamento è soggetto a revisione con frequenza annuale.