

# **Comune di Maruggio**

Provincia di TARANTO

## **Disposizioni per la sicurezza e l'utilizzo degli strumenti informatici**

**APPROVATO CON DELIBERA DI G.C. N. 85 DEL 12/05/2008**

## Premessa

Le informazioni sono un bene che ha un valore per l'Ente e, di conseguenza, necessita di essere protetto adeguatamente.

Le informazioni possono essere presenti in molte forme. Possono essere stampate o scritte su carta, memorizzate elettronicamente, trasmesse per posta o utilizzando altri mezzi elettronici, visualizzate su pellicole o trasmesse in una conversazione. Qualunque forma abbiano le informazioni o qualunque sia il mezzo su cui è condivisa o memorizzata una informazione, questa dovrebbe essere sempre protetta adeguatamente.

La sicurezza delle informazioni è definita qui come il mantenimento della:

- a) **riservatezza**: l'assicurazione che le informazioni siano accessibili solo a coloro che sono autorizzati ad avere l'accesso;
- b) **integrità**: salvaguardare la precisione e la completezza dell'informazione e del metodo di elaborazione;
- e) **disponibilità**: l'assicurazione che gli utenti autorizzati abbiano accesso alle informazioni e ai beni quando richiesto.

La sicurezza delle informazioni è ottenuta realizzando un insieme adatto di controlli, che potrebbero essere criteri, pratiche, procedure, strutture organizzative e funzioni software.

Inoltre la progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete Internet dai Personal Computer, espone l'organizzazione ai rischi di un coinvolgimento sia patrimoniale che penale, creando problemi alla sicurezza e all'immagine dell'Ente stesso.

Premesso che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente sono basilari in un rapporto di lavoro, l'Ente ha adottato il presente regolamento per contribuire alla massima diffusione della cultura della sicurezza ed evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.

Il Regolamento di seguito riportato viene incontro quindi alla necessità di disciplinare le condizioni per il corretto utilizzo degli strumenti informatici da parte dei dipendenti e contiene informazioni utili per comprendere cosa può fare ogni dipendente per contribuire a garantire la sicurezza informatica di tutto l'Ente.

Tale prescrizione si aggiunge e integra le norme già previste dal contratto di lavoro nonché dal "Documento Programmatico sulla Sicurezza" adottato dall'Ente.

Infine questo regolamento viene adottato alla luce del Provvedimento a carattere generale emesso Garante per la protezione dei dati personali il 1° marzo 2007, relativo all'utilizzo della posta elettronica e della rete Internet nel rapporto di lavoro.

# **Regole per l'utilizzo degli strumenti informatici**

## **1. Utilizzo dei personal computer**

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.

Il personal computer (PC) affidato al dipendente è uno strumento di lavoro. Ognuno 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.

Non è consentita l'attivazione della password d'accensione (bios), senza preventiva autorizzazione da parte dell'Ente.

Quasi tutti i PC trattano dati personali. Pertanto 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.

Il Titolare, anche attraverso personale delegato, ha la facoltà in qualunque momento di accedere ai dati trattati da ciascuno.

Non è consentito installare autonomamente programmi provenienti dall'esterno salvo previa autorizzazione esplicita del Titolare/Responsabile, previa consultazione del Responsabile della sicurezza (se designato), perché sussiste il grave pericolo di portare virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore.

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.

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

L'amministratore di sistema (o altra figura delegata dal Titolare) 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.

Non è consentito all'utente modificare le caratteristiche impostate sul proprio PC, salvo previa autorizzazione esplicita del Titolare o figura delegata.

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.

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 della direzione o figura delegata.

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.

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 del presente Regolamento relativo alle procedure di protezione antivirus.

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.

Devono essere prontamente segnalati per iscritto alla Segretario/Direttore generale:

- Il furto
- Il danneggiamento o lo smarrimento degli strumenti informatici
- Ogni malfunzionamento hardware e software (nel caso che il servizio di manutenzione sia esternalizzato vanno utilizzati i moduli predisposti dall'azienda affidataria del servizio).

Il Segretario/Direttore generale 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.

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 Titolare/Responsabile (o altro custode della password designato) in base alla modalità descritte nelle istruzioni operative.

## **2. Uso della rete Aziendale (Intranet)**

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 (anche soggetti esterni).

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.

Per garantire la manutenzione della sicurezza e della rete, soggetti autorizzati dal Segretario/Direttore generale (di norma Amministratori di sistema e aziende esterne autorizzate) possono monitorare gli apparati, i sistemi ed il traffico in rete in ogni momento rispettando la riservatezza degli utilizzatori attraverso analisi aggregata ed anonima dei dati di traffico.

Controlli su base individuale saranno attivati solo in caso di reiterati comportamenti illeciti e non conformi e comunque dopo un avviso generalizzato relativo al rilevato utilizzo anomalo degli strumenti aziendali.

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' 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.

Qualora si verificano 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.

Non è consentito collegare sistemi informatici di soggetti terzi esterni se non con l'autorizzazione espressa del Segretario/Direttore generale. Assicurarsi che i sistemi di soggetti terzi, esterni, qualora interagiscano con il sistema informatico dell'Ente, siano dotati di adeguate misure di protezione antivirus.

### **3. Utilizzo delle credenziali di autenticazione e gestione delle password (parola chiave)**

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.

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

Le credenziali di autenticazione devono essere disattivate:

- se non utilizzate da almeno sei mesi, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica;
- in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

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.

Il custode delle parole chiave (password) se non è nominato specificatamente coincide con il proprio responsabile dell'ufficio (in mancanza con il Titolare).

La comunicazione al custode delle parole chiave avviene secondo le seguenti modalità:

- 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;
- Chiuse in busta.

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.

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.

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

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.

#### **4. Utilizzo dei supporti rimovibili**

I supporti rimovibili contenenti dati sensibili, giudiziari o di natura riservata 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 alcun modo ricostruibili.

I supporti magnetici contenenti dati sensibili, giudiziari o di natura riservata devono essere custoditi in archivi controllati (chiusi a chiave,.....).

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

#### **5. Utilizzo di personal computer portatili**

L'utente è responsabile del PC portatile assegnategli dall'Ente e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

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.

I PC portatili utilizzati all'esterno (convegni, visite in azienda), in caso di allontanamento, devono essere custoditi in un luogo protetto.

Il portatile non deve essere mai lasciato incustodito e sul disco devono essere conservati solo i files strettamente necessari.

#### **6. Uso della rete Internet e dei relativi servizi**

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.

Non è consentito:

- l'accesso a siti inappropriati (esempio siti pornografici, di intrattenimento,

etc) e lo scarico (download) di software o di file non necessari all'attività aziendale;

- utilizzare programmi per la condivisione e lo scambio di file in modalità peer to peer (Nasper, Emule, Winmx, e-Donkey, ecc);
- accedere a flussi in streaming audio/video da Internet per scopi non attinenti all'attività lavorativa (ad esempio ascoltare la radio o guardare video o filmati utilizzando le risorse Internet).

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.

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

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).

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'organizzazione (o suo responsabile delegato).

Per garantire la manutenzione della sicurezza e della rete, soggetti autorizzati dal Segretario/Direttore Generale (di norma Amministratori di sistema e aziende esterne autorizzate) possono monitorare gli apparati, i sistemi ed il traffico in rete in ogni momento rispettando la riservatezza degli utilizzatori attraverso analisi aggregata ed anonima dei dati di traffico.

Controlli su base individuale saranno attivati solo in caso di reiterati comportamenti illeciti, anomali o non conformi alla normativa e al presente regolamento, e comunque dopo un avviso "generalizzato" relativo al rilevato utilizzo anomalo degli strumenti aziendali all'intera struttura lavorativa o sue aree.

## **7. Uso della posta elettronica**

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'Ente. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

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.

La posta elettronica resta comunque un bene dell'Ente, come tale accessibile ai soggetti autorizzati e al datore di lavoro.

E' necessario inserire nei messaggi un avvertimento ai destinatari nel quale sia dichiarata l'eventuale natura non personale del messaggio e sia specificato che le risposte potranno essere conosciute dall'organizzazione di appartenenza del mittente.

Non esiste un diritto all'utilizzo esclusivo da parte dell'utente di una casella di posta elettronica, pertanto in caso di necessità l'Ente si riserva il diritto, in

qualità di proprietario del bene, di accedere al contenuto della casella di posta, di riassegnare l'uso della casella di posta ad altro utente, di effettuare controlli sull'uso.

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.

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.

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

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).

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

## **8. Protezione antivirus**

Tutti i PC, i server ed i sistemi di elaborazione in genere, che sono connessi in rete interna dell'Azienda (intranet) e/o esterna (internet/extranet) di proprietà dell'Ente o del personale, devono essere dotati di un sistema antivirus approvato dal Segretario/Direttore Generale ed aggiornato.

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

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.

Nel caso che il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente:

- a) sospendere ogni elaborazione in corso senza spegnere il computer;
- b) segnalare l'accaduto al responsabile della sicurezza (se designato).

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

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 al responsabile della sicurezza.

## **9. Utilizzo delle stampanti e dei materiali di consumo**

L'utilizzo delle stampanti e dei materiali di consumo in genere (carta, inchiostro, toner, floppy disk, supporti digitali come CD e DVD) è riservato esclusivamente ai compiti di natura strettamente amministrativa. Devono essere evitati in ogni modo sprechi dei suddetti materiali o utilizzi eccessivi.

## **Norme conclusive**

### **10. Non osservanza del regolamento**

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.

### **11. Aggiornamento e revisione**

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Le proposte vanno esaminate dal Segretario/Direttore Generale.

Il presente Regolamento è soggetto a revisione con frequenza annuale.

