COMUNE DI ALBANO LAZIALE

(Provincia di Roma)

Regolamento per l'utilizzo degli strumenti informatici e telematici

INDICE ANALITICO

PREMESSA

La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete Internet dai Personal Computer, espone il Comune di Albano Laziale ai rischi di un coinvolgimento sia patrimoniale che penale, creando problemi alla sicurezza e all'immagine.
Inoltre le recenti disposizioni emanate dall'Autorità Garante, mediante il provvedimento di carattere generale del 1 Marzo 2007 (Del. N. 13 del 1/3/2007), in cui vengono definite le linee guida per l'utilizzo della posta elettronica ed Internet impongono l'adozione di precise e definite regole per l'utilizzo di tali strumenti.
Premesso infine che:

- l'utilizzo delle risorse informatiche e telematiche del Comune di Albano Laziale deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro, per questi è adottato un Regolamento Informatico interno, diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati;

- compete al datore di lavoro assicurare le funzionalità ed il corretto impiego di tali mezzi da parte dei lavoratori, definendone le modalità d'uso nell'organizzazione dell'attività lavorativa, tenendo conto della disciplina in termini di diritto del lavoro;

le prescrizioni che seguono sono formulate in attuazione del D.Lgs. N°196/2003 e successive modifiche ed integrazioni, sulle misure di sicurezza obbligatorie ed in rispondenza a quanto evidenziato nel provvedimento del 1/3/2007 su citato.

1. UTILIZZO DEL PERSONAL COMPUTER

I.I. Il Personal Computer (in avanti, per brevità, PC) affidato a ciascun dipendente (per tale dovendosi intendere una persona che ha un qualunque rapporto di lavoro con il Comune di Albano Laziale non necessariamente e non solo a tempo indeterminato) o a chiunque comunque lo utilizzi a vario titolo**,** è da considerare uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza, e pertanto si fa divieto di utilizzo per attività non inerenti al rapporto lavorativo.

1.2. L'accesso al PC è protetto da password che deve essere custodita dall'incaricato con la massima diligenza e non divulgata se non al custode della password con le modalità definite dal Documento Programmatico per la Sicurezza vigente. 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 , o da un suo delegato per atto scritto, o chi ne fa le funzioni, non essendo attualmente presente nell'organico una figura professionale a cui attribuire tale denominazione (in avanti per brevità sarà riportato Amministratore del Sistema)

1.3. L'Amministratore del Sistema, per l'espletamento delle sue funzioni o per esigenze produttive ed organizzative (ad es. per rilevare anomalie o per manutenzioni del sistema) o per esigenze connesse alla sicurezza dell'attività lavorativa, può avvalersi legittimamente, nel rispetto dello Statuto del Lavoratori (art. 4, comma 2), di sistemi che consentono indirettamente un controllo a distanza (c.d. controllo preterintenzionale), che determinano un trattamento di dati riferiti o riferibili ai lavoratori. Tale trattamento sarà operato nel rispetto delle procedure di informazione e consultazione dei lavoratori.

1.4. Non è consentito installare autonomamente programmi, salvo quanto autorizzato per iscritto dell'Amministratore del Sistema, in quanto sussiste il grave pericolo di introdurre Virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore e di conseguenza dell'intero sistema in rete. Inoltre non è consentito l'uso di programmi diversi da quelli distribuiti ufficialmente dal Comune di Albano Laziale (dlg. 518/92 sulla tutela giuridica del software e L. 248/2000 nuove norme di tutela del diritto d'autore).

1.5. Non è consentito all'utente modificare le caratteristiche impostate sul proprio PC, salvo autorizzazione scritta dell'Amministratore del Sistema.

1.6. Il PC deve essere spento ogni sera prima di lasciare gli uffici e in caso di allontanamento dalla propria postazione di lavoro, deve essere attivato lo screen saver e la relativa password, onde impedirne l'indebito uso da parte di terzi.

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

1.8. Ai dipendenti incaricati del trattamento dei dati sensibili è fatto divieto l'accesso contemporaneo con lo stesso account da più PC.

1.9. Chiunque utilizzi i PC 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 punto 8 del presente Regolamento relativo alle procedure di protezione antivirus.

1.10. 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, politica e/o filosofica.

2. UTILIZZO DELLA RETE INFORMATICA DEL COMUNE DI ALBANO LAZIALE

2.1. 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. Sulle stesse, vengono svolte regolari attività di controllo, amministrazione e backup da parte dell'Amministratore del Sistema, e dagli incaricati individuati da quest'ultimo con atto scritto.

2.2. L'Amministratore del Sistema, può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza e la funzionalità sia dei singoli PC degli incaricati, che delle unità di rete condivise.

2.3. Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutilizzati. Particolare attenzione deve essere prestata alla duplicazione dei dati, è infatti, assolutamente da evitare un'archiviazione ridondante ed i relativi sistemi di back-up devono essere configurati in modo da cancellare periodicamente ed automaticamente (attraverso procedure di sovra registrazione) i dati precedentemente memorizzati.

2.4. E' cura dell'utilizzatore 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 file di contenuto grafico) su stampanti comuni. In caso di necessità la stampa in corso può essere cancellata.

3. GESTIONE DELLE PASSWORD

3.1. Le password di ingresso alla rete, di accesso ai programmi e dello screen saver, sono previste ed attribuite inizialmente dall'Amministratore del Sistema. E' obbligatoria al primo utilizzo l'autonoma sostituzione della password da parte del/i dipendente/i il quale dovrà provvedere alla consegna della stessa in busta chiusa e controfirmata sui lembi laterali al Custode delle Password. L'Amministratore di Sistema, dopo l'autonoma sostituzione della password da parte del dipendente, non sarà più a conoscenza di questa, ma ha facoltà di resettarla per motivi di servizio. In caso di cancellazione della password, l'Amministratore di Sistema comunicherà la cancellazione della medesima al dipendente interessato, che provvederà a una nuova autonoma obbligatoria sostituzione, prima di iniziare a utilizzare la postazione a sua disposizione. Nel caso in cui il sistema lo consenta, l'Amministratore di Sistema, utilizzerà gli automatismi di richiesta di cambio password in luogo della comunicazione al dipendente, in funzione degli intervalli di sostituzione richiesti dalla normativa.

3.2. La password, quando e' prevista dal sistema di autenticazione, e' composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito.
Essa non deve contenere riferimenti agevolmente riconducibili al dipendente (non solo nomi, cognomi, soprannomi, ma neppure date di nascita, proprie, dei figli o degli amici), né consistere in nomi noti, anche di fantasia (pippo, pluto, paperino, pippobaudo….), buona norma è che, dei caratteri che costituiscono la password, da un quarto alla metà siano di natura numerica.
La password è modificata obbligatoriamente dal dipendente incaricato al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave deve essere modificata almeno ogni tre mesi.

3.3. Chiunque venisse a conoscenza di altre password, è obbligato a darne immediata notizia al Responsabile della Sicurezza del settore di appartenenza e all'Amministratore del Sistema .

4. UTILIZZO DEI SUPPORTI DI MEMORIZZAZIONE REMOVIBILI

4.1. I supporti removibili non devono contenere dati sensibili o giudiziari. I supporti removibili, se non utilizzati, sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri dipendenti se le informazioni precedentemente in essi contenute non sono intelligibili e, tecnicamente, in alcun modo ricostruibili.

4.2. Non è consentito scaricare files contenuti in supporti removibili non aventi alcuna attinenza con la propria attività lavorativa.

4.3. Tutti i files di provenienza incerta od esterna, ancorché attinenti all'attività lavorativa, devono essere sottoposti al controllo ed alla relativa autorizzazione all'utilizzo da parte dell'Amministratore del Sistema.

4.4. Ogni dispositivo magnetico di provenienza esterna al Comune di Albano Laziale dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, il supporto dovrà essere consegnato all'Amministratore di Sistema.

5. UTILIZZO DI PC PORTATILI

5.1. Laddove esistente, il dipendente è responsabile del PC portatile assegnatogli e deve custodirlo con estrema diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

5.2. 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.

5.3. I PC portatili utilizzati all'esterno (convegni, incontri, meeting ecc.), in caso di allontanamento, devono essere custoditi in un luogo protetto.

5.4. Quanto stabilito al punto 5.3. si estende a tutti e ad ogni apparecchio elettronico ceduto in uso dal Comune di Albano Laziale al dipendente.

6. USO DELLA POSTA ELETTRONICA

6.1. La casella di posta elettronica, assegnata dal Comune di Albano Laziale al dipendente, o ad altra figura all'interno dell'Amministrazione, è uno strumento di lavoro. Gli assegnatari delle caselle di posta elettronica sono responsabili personalmente del contenuto e del corretto utilizzo delle stesse.

6.2. E' fatto divieto di utilizzare le caselle di posta elettronica del Comune di Albano Laziale, per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list non attinenti all'attività lavorativa, salvo diversa autorizzazione scritta dell'Amministratore del Sistema.

6.3. E' fatto divieto inviare e/o ricevere 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.

6.4. Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per il Comune di Albano Laziale, ovvero contenga documenti da considerarsi riservati in quanto contraddistinti dalla dicitura "Riservato/i" o “Riservato/i personale/i” o analoga dicitura, deve essere visionata od autorizzata dal nominato Responsabile della Sicurezza del Settore di appartenenza.

6.5. E' possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario, ma per la comunicazione ufficiale è obbligatorio avvalersi degli strumenti tradizionali (fax, posta) anche se alle e-mail è stato riconosciuto valore probatorio, o fino al momento in cui le e-mail saranno ritenute sicure e non modificabili.

6.6. Per la trasmissione di file all'interno del Comune di Albano Laziale, è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati.

6.7. 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).

6.8. E' vietato inviare catene telematiche (o di Sant'Antonio). Se si dovessero ricevere messaggi di tale tipo, deve essere comunicarlo immediatamente all'Amministratore del Sistema. Non si deve in alcun caso attivare gli allegati di tali messaggi.

6.9. Saranno messe a disposizione dei singoli incaricati le funzionalità del software di gestione della posta elettronica, che consentiranno, qualora ci dovessero essere assenze programmate, di inviare, in automatico, messaggi di risposta che contengano le “coordinate” di altro soggetto o strutture della Comune di Albano Laziale operanti al posto del lavoratore assente.

6.10. Qualora dovesse rendersi necessario conoscere il contenuto dei messaggi di posta elettronica in caso di assenza prolungata od improvvisa e/o per improrogabili necessità legate all’attività lavorativa, l’incaricato dovrà individuare un proprio collega “fiduciario” il quale provvederà a verificare il contenuto dei messaggi e ad inoltrare al Responsabile della Sicurezza quelli ritenuti rilevanti per lo svolgimento dell’attività lavorativa. Di tale attività sarà redatto un verbale ed informato tempestivamente alla prima occasione utile il lavoratore interessato.

6.11. Si ritiene necessario che ciascun incaricato introduca nei propri messaggi di posta elettronica, uno specifico avvertimento ai destinatari nel quale sia dichiarata l’eventuale natura non personale del messaggio e sia specificato se le risposte potranno essere conosciute nell’organizzazione di appartenenza del mittente, rimandando a questo specifico Regolamento informatico.

6.12. Si evidenzia che, qualora dovessero rendersi necessari dei controlli sull’uso degli strumenti elettronici da parte dei lavoratori saranno rispettati i principi di pertinenza e non eccedenza e saranno evitate ingiustificate interferenze sui diritti e sulle libertà fondamentali dei lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata. In tal senso eventuali

esigenze connesse ad azioni mirate di controllo saranno effettuate in maniera graduale, riguardando in prima istanza dati aggregati, riferiti all'intera struttura lavorativa o sue specifiche aree, richiamando le stesse ad utilizzo pertinente degli strumenti informatici posti a loro disposizione. Qualora gli esiti dovessero generare l'assenza di successive anomalie saranno effettuati controlli di carattere generale.
Si precisa altresì che tali controlli non saranno effettuati in maniera prolungata, costante o indiscriminata, ma mirati ad individuare eventi dannosi o situazioni di pericolo per le quali non sia stato possibile impedirne gli effetti attraverso preventivi accorgimenti tecnici.

7. USO DELLA RETE INTERNET E DEI RELATIVI SERVIZI

7.1. Il PC abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa

7.2. E' vietata la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa. A maggior ragione non è consentito navigare in siti che accolgono contenuti contrari alla morale e alle prescrizioni di Legge.
Non è inoltre consentito navigare in siti che possano rilevare la profilazione dell'individuo definita "sensibile " ai sensi del D. Lgs. 196/2003: quindi siti la cui navigazione palesi elementi attinenti alla fede religiosa, alle opinioni politiche, filosofiche e sindacali del dipendente o le sue abitudini sessuali.

7.3. E' fatto divieto al dipendente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dall'Amministratore del Sistema.

7.4. Non è consentito lo scarico di materiale elettronico tutelato dalle normative sul Diritto d'Autore (software, file audio, film, etc.) né attraverso Internet, né attraverso servizi peer-to-peer.

7.5. E' tassativamente vietata l'effettuazione per uso privato di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line, prenotazioni e simili.

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

7.7. E' vietata la partecipazione a Forum non professionali, l'utilizzo di chat (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).

7.8. 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.

7.9. Si evidenzia che, qualora dovessero rendersi necessari dei controlli sull'uso di Internet da parte dei lavoratori, saranno rispettati i principi di pertinenza e non eccedenza e saranno evitate ingiustificate interferenze sui diritti e sulle libertà fondamentali dei lavoratori. In tal senso eventuali esigenze connesse ad azioni mirate di controllo saranno effettuate in maniera graduale, riguardando in prima istanza dati aggregati, riferiti all'intera struttura lavorativa o gruppi sufficientemente ampi di lavoratori tali da precludere l'immediata identificazione degli utenti (ad es., con riguardo ai *file* di *log* riferiti al traffico).
Si precisa altresì che tali controlli non saranno effettuati in maniera prolungata, costante o indiscriminata, ma mirati ad individuare eventi dannosi o situazioni di pericolo per le quali non sia stato possibile impedirne gli effetti attraverso preventivi accorgimenti tecnici. In tal senso il Comune di Albano Laziale provvederà ad individuare ed installare dei software (detti comunemente web filter) che prevengano determinate operazioni, reputate inconferenti con l'attività lavorativa, quali l'upload o l'accesso a determinati siti (inseriti in una sorta di black list) e/o il download di file o software aventi particolari caratteristiche (dimensionali o di tipologia di dato).

7.10. La conservazione dei dati riguardanti l'uso degli strumenti elettronici è regolata in modo che venga automaticamente effettuata la sovraregistrazione dei file, e vengano in tal maniera cancellati periodicamente ed automaticamente i dati personali la cui conservazione non sia necessaria.
Un eventuale prolungamento dei tempi di conservazione va valutato come eccezionale e può aver luogo solo in relazione :
- ad esigenze tecniche o di sicurezza del tutto particolari
- all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria
- all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

8. PROTEZIONE ANTIVIRUS

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

8.2. Ogni utilizzatore di PC è tenuto a controllare il regolare funzionamento del software installato, segnalandone immediatamente il cattivo funzionamento all'Amministratore del Sistema.

8.3. Nel caso che il software antivirus rilevi la presenza di un virus, il dipendente dovrà immediatamente: a) sospendere ogni elaborazione in corso senza spegnere il computer;
b) interrompere immediatamente il traffico di rete ed internet;
c) segnalare l'accaduto all'Amministratore del Sistema.

9. OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PRIVACY

9.1. E' obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza, come indicate nella lettera di individuazione di incaricato del trattamento dei dati ai sensi del D Lgs. N°196/2003. Il presente Regolamento integra il Documento Programmatico della Sicurezza (DPS) vigente adottato dalla Comune di Albano Laziale.

10. NON OSSERVANZA DEL REGOLAMENTO INFORMATICO

10.1. Il mancato rispetto o la violazione delle regole contenute nel presente regolamento sono perseguibili con provvedimenti disciplinari nonché con le azioni civili e penali consentite dalla legge che il Comune di Albano Laziale riterrà di avviare.