RESPONSABILE SETTORE I.C.T.
DOTT. SERGIO MASSAINI

COMUNE DI CIVITA CASTELLANA

(Prov. di Viterbo)

REGOLAMENTO COMUNALE PER LA SICUREZZA

E L'UTILIZZO DELLE PDL

(POSTAZIONI DI LAVORO)

PREMESSA

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

Premesso che l'utilizzo delle risorse informatiche e telematiche comunali deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente sono basilari in un rapporto di lavoro, l'Amministrazione Comunale ha adottato il presente regolamento, sollecitato e redatto dal Responsabile Settore I.C.T., alla luce del "Documento Programmatico sulla Sicurezza", 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 aziendale 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 del Comune.

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

INDICE

1. UTILIZZO DELLE PDL POSTAZIONI DI LAVORO : **MONITOR, CPU, TASTIERA, MOUSE, STAMPANTE, TELEFONO.**

1.1. Ad ogni dipendente è assegnata una PDL quale strumentazione 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, con individuazione della responsabilità oggettiva.

1.2. Non è consentita l'attivazione della password d'accensione (bios), senza preventiva autorizzazione da parte del Responsabile Settore I.C.T.

1.3. Non è consentito all'utente modificare le caratteristiche hardware e software impostate sul proprio PC, salvo previa autorizzazione esplicita da parte del Responsabile Settore I.C.T.

1.4. Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio.

1.5. Le informazioni archiviate in formato digitale devono essere esclusivamente quelle previste dalla legge o necessarie all'attività lavorativa.

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

1.7. La tutela della gestione locale di dati su postazioni di lavoro individuali, dispositivi mobili, personal computer che gestiscono localmente documenti e/o dati – nel rispetto della Privacy è demandata all'utente finale che dovrà effettuare, con frequenza opportuna, i salvataggi di backup.

E' comunque vietato l'uso di supporti di archiviazione removibili per la memorizzazione dei dati, per ogni necessità di archiviazione di dati sensibili contattare il Responsabile I.C.T. che renderà disponibili archivi protetti.

1.8. Le gestioni locali dei dati non è più consentita, il dato deve essere gestito sul server in modo centralizzato con Active Directory. E' consentita deroga per programmi di posta elettronica e altri software che hanno il database installato sul client che non permettono archiviazione sul server.

1.9. Non è consentita l'installazione di programmi diversi da quelli Installati, ulteriori installazioni devono essere autorizzate dal Responsabile del Settore I.C.T.

1.10. Non è consentita la riproduzione o la duplicazione di programmi informatici ai sensi delle Legge n.128 del 21.05.2004.

1.11. Il Responsabile Settore I.C.T. potrà in qualunque momento procedere alla rimozione di ogni file o applicazioni che riterrà essere pericolosi per la Sicurezza sia sui PC degli incaricati, sia sulle unità di rete.

2. UTILIZZO DELLA RETE DELL'AMMINISTRAZIONE COMUNALE

2.1 L'accesso alla rete aziendale è protetto da password; per l'accesso deve essere utilizzato il proprio profilo personale (username e password).

2.2 E' fatto divieto di utilizzare la rete aziendale per fini non espressamente autorizzati.

2.3 E' vietato connettere in rete stazioni di lavoro se non dietro esplicita e formale autorizzazione del Responsabile del Settore I.C.T.

2.4 E' vietato condividere cartelle in rete sia dotate di password, sia sprovviste di password se non dietro esplicita e formale autorizzazione del Responsabile del Settore I.C.T.

2.5 E' vietato monitorare ciò che transita in rete.

2.6 E' vietata l'installazione non autorizzata di modem che sfruttino il sistema di comunicazione telefonico che l'abilitazione e l'apertura di accessi remoti a banche dati esterne o interne all'azienda.

3. GESTIONE DELLE PASSWORD.

3.1 Le password d'ingresso alla rete, di accesso ai vari programmi in rete per i trattamenti dei dati e ad Internet, sono attribuite dal Responsabile Settore I.C.T. Al riguardo è individuato un modulo di "Concessione /Revoca/Modifica abilitazioni applicative" che i responsabili dei trattamenti utilizzeranno per le comunicazioni del caso al Responsabile Settore I.C.T.

3.2 L'utente è tenuto a conservare nella massima segretezza la parola di accesso alla rete ed ai sistemi e qualsiasi altra informazione legata al processo di autenticazione.

3.3 L'utente è tenuto a scollegarsi dal sistema ogni qualvolta sia costretto ad assentarsi dal locale nel quale è ubicata la stazione di lavoro o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima: 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.

3.4 La password deve essere immediatamente sostituita, dal Responsabile Settore I.C.T., nel caso si sospetti che la stessa abbia perso la segretezza.

4. UTILIZZO DI DISPOSITIVI MOBILI.

4.1 L'utente è responsabile del dispositivo mobile assegnatogli dall'Azienda e deve custodirlo con diligenza, sia durante gli spostamenti, sia durante l'utilizzo nel luogo di lavoro.

4.2 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.

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

4.4 II dispositivo mobile non deve essere mai lasciato incustodito e sul disco devono essere conservati solo i files strettamente necessari.

4.5 Nel caso di accesso alla rete aziendale tramite Terminal Server (Remote Access Server) / Accesso Remoto: utilizzare l'accesso in forma esclusivamente personale utilizzare la password in modo rigoroso.

4.6 Disconnettersi dal sistema Terminal Server al termine della sessione di lavoro.

4.7 Collegarsi periodicamente alla rete interna per consentire il caricamento dell'aggiornamento dell'anti virus.

4.8 Non utilizzare connessioni Internet privati per collegamenti alla rete, l'accesso ad internet deve avvenire soltanto tramite il Gateway predefinito.

4.9 L'utilizzo di supporti di archiviazione rimovibili non è ammesso, l'utilizzo deve essere preventivamente autorizzato dal Responsabile del Settore I.C.T.

5. USO DELLA POSTA ELETTRONICA.

5.1. L'assegnazione di una casella di posta elettronica deve essere preceduta da regolare richiesta del Responsabile di Area, al Responsabile I.C.T. il quale avvierà la procedura abilitativa ne seguirà la relativa attivazione nei tempi tecnici necessari.

5.2. La casella di posta, assegnata dall'Amministrazione all'utilizzatore, è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili in proprio delle conseguenze derivanti al non corretto utilizzo delle stesse (art. 615 comma 5 e segg. c.p.) .

5.3. Nel caso di mittenti sconosciuti o messaggi insoliti, per non correre il rischio di essere infettati da virus occorrerà cancellare i messaggi senza aprirli.

5.4. Nel caso di messaggi provenienti da mittenti conosciuti ma che contengono allegati sospetti (file con estensione .zip .exe .scr .pif .bat .cmd), questi ultimi non devono essere aperti.

5.5. L'utilizzo della posta personale sulle postazioni di lavoro non è consentita.

5.6. Evitare che la diffusione incontrollata di "Catene di Sant'Antonio" (messaggi a diffusione capillare e moltiplicata) limiti l'efficienza del sistema di posta.

5.7. Utilizzare, nel caso di invio di allegati pesanti, i formati compressi (*.zip *.rar *.jpg).

5.8. Nel caso in cui si debba inviare un documento all'esterno dell'Azienda è preferibile utilizzare un formato protetto da scrittura.

5.9. L'iscrizione a "mailing list" esterne è concessa solo per motivi professionali, prima di iscriversi occorre verificare in anticipo se il sito è affidabile.

5.10. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

5.11. Per la trasmissione di file all'interno dell'Amministrazione è possibile utilizzare sia la rete LAN che la posta elettronica, prestando attenzione alla dimensione degli allegati che non devono mai superare i 5 MB.

5.12. 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. USO DELLA RETE INTERNET E DEI RELATIVI SERVIZI.

6.1 L'abilitazione alla posta esterna e ad Internet deve essere preceduta da regolare richiesta del Responsabile di Area al RESPONSABILE SETTORE I.C.T.

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

6.3 E' assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.

6.4 Non possono essere utilizzati dispositivi privati per il collegamento alla rete.

6.5 E' fatto divieto all'utente lo scarico di software sulla postazione, qualsiasi sia la provenienza "con particolare attenzione a SW gratuito, freeware e/o shareware prelevato da siti Internet", di cui non sia verificata l'impronta hash ed espressamente autorizzato dal RESPONSABILE SETTORE I.C.T.

6.6 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).

7 PROTEZIONE ANTIVIRUS.

7.1 Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo (ad esempio non aprire mail o relativi allegati sospetti, non navigare su siti non professionali ecc..), si chiede di prestare particolare attenzione alle comunicazioni di allerta del SETTORE I.C.T. via e-mail, su cosa fare in tali casi di attacco.

7.2 Ogni utente è tenuto a controllare la presenza e il regolare funzionamento del software antivirus aziendale.

7.3 Nel caso che il software antivirus rilevi la presenza di un virus che non è riuscito a ripulire, l'utente dovrà immediatamente sospendere ogni elaborazione in corso, scollegare il cavo LAN e spegnere il computer, segnalare l'accaduto al RESPONSABILE SETTORE I.C.T.

7.4 Ogni dispositivo magnetico/ottico/USB di provenienza esterna all'azienda dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus non eliminabile dal software, non dovrà essere utilizzato.

7.5 Il RESPONSABILE SETTORE I.C.T. ha predisposto una specifica casella di posta elettronica denominata services@comune.civitacastellana.vt.it a cui inviare notizie di anomalie o problematiche varie, tra cui virus ed antivirus.

8 OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PRIVACY

8.1 E' obbligatorio attenersi alle disposizioni previste dal D.Lgs 30 giugno 2003 n° 196 e s.m.i, tra cui le Linee guida in materia di trattamento di dati personali per finalità di pubblicazione e diffusione di atti e documenti di enti locali 19 aprile 2007, G.U. n. 120 del 25 maggio 2007, al Documento Programmatico sulla Sicurezza, al presente Regolamento sulle misure minime di sicurezza ed al contratto di lavoro del Pubblico Impiego.

9 NON OSSERVANZA DELLA NORMATIVA AZIENDALE.

9.1 Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali previste dalle leggi (art. 171-ter L 633/1941, L 248/00, art. 547 c.p. - art.594 e 595 c.p. - art. 600-ter e seg. c.p.- art. 615 ter c.p.- art. 615 quater c.p. - art. 615- quinques c.p.- art. 617 quater c.p.- art. 617 quinquies c.p. - art. 617 sexies c.p. - art. 635- bis c.p.- art. 640 e 640 ter c.p.).

10 AGGIORNAMENTO E REVISIONE

10.1 Tutti gli utilizzatori possono proporre, quando ritenuto necessario, integrazioni al presente regolamento tramite comunicazione al Responsabile Settore I.C.T.

10.2 Il presente Regolamento è oggetto a revisione triennale

11 ENTRATA IN VIGORE

11.1 Il presente Regolamento entra in vigore il giorno successivo a quello della pubblicazione per 15 giorni all'Albo Pretorio del Comune.