Comune di Crotone

Allegato alla delibera GC n. 269 del 20.06.2007

Regolamento per la sicurezza e l'utilizzo delle postazioni di informatica sul luogo di lavoro

Rev. 0	Preparato:	Verificato:	Approvato:
11.06.2007	servizio Ced ing. Francesco De Raffaele	Giunta Comunale	con delibera di G.C. n.

Sommario

Articolo I. Finalità e campo di applicazione

Il Regolamento di seguito riportato viene incontro 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, dal "Piano programmatico sulla sicurezza informatica" (DPS) già adottato dal Comune di Crotone e tiene conto delle direttive impartite dal Garante per la tutela del dipendente durante il proprio lavoro.

Tra il personale del comune di Crotone sono compresi tutti coloro che svolgono attività lavorative per il comune, con contratto a tempo indeterminato, determinato, con forme di collaborazione coordinata e continuativa, con forme di lavoro interinale e con ogni altra forma contrattuale che si trovino, anche occasionalmente, nella condizione di dover utilizzare le attrezzature informatiche di proprietà dell'ente.

Il regolamento si applica anche ai consiglieri comunali, agli assessori ed agli organi di staff di cui al Decreto legislativo 267/2000.

Articolo II. Utilizzo del Personal Computer

Il Comune di Crotone mette a disposizione dei dipendenti le strumentazioni informatiche necessarie per lo svolgimento delle attività lavorative. Gli stessi diventano responsabili delle strumentazioni durante il loro utilizzo.

Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

Non è consentito all'utente modificare le caratteristiche hardware e software impostate sul proprio Personal Computer (PC), salvo autorizzazione esplicita da parte del responsabile del Servizio Informatico (SI) dell'Ente.

Tutte le attrezzature informatiche devono essere spente prima di allontanarsi dalla propria postazione sia in caso di assenza prolungata che al termine del processo lavorativo.

Le informazioni archiviate informaticamente devono essere esclusivamente quelle previste dalla legge o necessarie all'attività lavorativa dall'ufficio.

La tutela della gestione locale dei dati su stazioni di lavoro personali è demandata all'utente finale che dovrà effettuare, con frequenza opportuna, i salvataggi su supporti magnetici e/o di rete e la conservazione degli stessi in luogo idoneo. E' comunque vietato l'uso di supporti di archiviazione removibili per la memorizzazione dei dati sensibili.

Non è consentita l'installazione di programmi diversi da quelli autorizzati dal SI dell'Ente.

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

Gli operatori del SI possono in qualunque momento procedere alla rimozione di ogni file o applicazione che riterranno essere pericolosi per la sicurezza sia sui PC degli incaricati sia sulle unità di rete.

Articolo III. Gestione delle Password.

L'accesso alla rete, l'uso degli strumenti elettronici e l'uso delle procedure informatiche per il trattamento di dati dell'Ente è consentito esclusivamente agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa ad uno specifico trattamento o a un insieme di trattamenti.

Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo.

Le credenziali di autenticazione d'ingresso alla rete, di accesso ai vari programmi in rete per i trattamenti dei dati e di accesso ad Internet, sono attribuite dagli addetti del SI dell'Ente e conservate in busta chiusa presso un luogo sicuro scelto dal responsabile della custodia delle credenziali.

L'utente è tenuto a non divulgare e conservare nella massima segretezza le credenziali di accesso alla rete ed ai sistemi e qualsiasi altra informazione legata al processo di autenticazione.

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 inseguito la possibilità di provarne l'indebito uso***.

La parola chiave deve essere immediatamente sostituita, dandone comunicazione al responsabile della custodia delle credenziali, nel caso si sospetti che la stessa abbia perso la segretezza.

La parola chiave è composta da almeno otto caratteri, non contiene riferimenti agevolmente riconducibili all'incaricato e deve essere modificata almeno ogni sei mesi.

Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate. Sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

In caso di eventuali assenze non programmate[1] il titolare del trattamento, perdurando l'assenza oltre un determinato limite temporale, può disporre lecitamente, sempre che sia necessario, dell'utilizzo delle credenziali di accesso per la visualizzazione dei dati memorizzati localmente sulla postazione di lavoro. E' cura del titolare del trattamento di tale attività redigere apposito verbale ed informare il lavoratore.

Non è consentita l'attivazione della password d'accensione (bios), senza preventiva autorizzazione da parte del SI e senza averla trascritta nell'apposita busta contenente le credenziali utilizzate.

Ulteriori disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione sono dettagliate nel Documento Programmatico di Sicurezza (DPS) adottato dall'Ente in ottemperanza al Decreto legislativo n. 196/2003 e riportate nella nomina ad Incaricato del trattamento dei dati consegnati all'utente.

Articolo IV. Profili di autorizzazione ed utilizzo della rete.

I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

I profili vengono assegnati dai Responsabili del trattamento dati su richiesta dei Dirigenti di settore e devono indicare con esattezza i dati che l'incaricato è autorizzato a trattare.

L'associazione fra profilo ed 'utente viene effettuato dagli addetti del SI.

Periodicamente, e comunque almeno annualmente, è verificata, dal SI, la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

---

[1] ad esempio per malattia

E’ obbligo dell’ufficio giuridico del personale comunicare tempestivamente ogni movimento che può modificare la sussistenza delle condizioni dei profili di autorizzazione.

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

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

E' fatto divieto di connettere in rete stazioni di lavoro se non dietro esplicita e formale autorizzazione del responsabile del SI.

E' fatto divieto di condividere cartelle in rete sia dotate di password sia sprovviste di password se non dietro esplicita e formale autorizzazione del responsabile del SI.

E’ fatto divieto di monitorare ciò che transita in rete, ed è vietata l'installazione non autorizzata di modem che sfruttino il sistema di comunicazione telefonico per l'accesso a banche dati esterne o interne all'azienda.

Articolo V. Utilizzo di PC portatili

L'utente è responsabile del PC portatile assegnatogli 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[2], 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.

L’utente provvederà a collegarsi periodicamente alla rete interna per consentire il caricamento dell'aggiornamento dell'antivirus.

[2] convegni, visite in azienda

Articolo VI. Uso della posta elettronica

L'Ente assegna ad ogni dipendente, amministratore e consigliere comunale, una casella di posta elettronica (email), legata al dominio dell'Ente, quale strumento di lavoro.

Le persone assegnatarie delle caselle di posta elettronica semplice e di Posta Elettronica Certifica (PEC) sono responsabili del corretto utilizzo delle stesse[3].

La posta elettronica può essere scaricata localmente attraverso l'uso di software appropriato ma che non richiede licenza d'uso diversa da quella già in possesso dell'Ente. Può essere gestita attraverso il servizio *webmail* usufruibile dal link presente sul sito istituzionale www.comune.crotone.it .

L'Ente, a richiesta dei responsabili di servizio, rende disponibile indirizzi di posta elettronica condivisi tra più dipendenti[4]. L'attivazione sarà a cura degli operatori del SI.

Il lavoratore può configurare, in accordo con gli addetti del SI la propria email con messaggi contenenti le "coordinate"[5] di un altro soggetto o altre utili modalità di contatto della struttura da inviare automaticamente in caso di assenze [6]

In caso di eventuali assenze non programmate (ad esempio per malattia), qualora il lavoratore non possa attivare la procedura descritta il titolare del trattamento, perdurando l'assenza oltre un determinato limite temporale, può disporre lecitamente, sempre che sia necessario e mediante personale appositamente incaricato, la visualizzazione dei messaggi di posta elettronica. L'interessato può delegare un altro lavoratore a verificare il contenuto di messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. E' cura del titolare del trattamento di tale attività, redigere apposito verbale e informare tempestivamente il lavoratore interessato.

---

[3] art. 615 comma 5 e segg. c.p.

[4] ad esempio reclami@comune.crotone.it, urp@ comune.crotone..it, etc.

[5] elettroniche o telefoniche

[6] ad es., per ferie o attività di lavoro fuori sede

I messaggi di posta elettronica devono contenere un avvertimento per i destinatari nel quale sia dichiarata l'eventuale natura non personale dei messaggi stessi, precisando che le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente.

Il lavoratore, nell'uso delle email, è tenuto ad osservare seguenti accorgimenti:

1. I messaggi provenienti da mittenti sconosciuti o messaggi insoliti, per non correre il rischio di essere infettati da virus, devono essere cancellati senza aprirli;
2. Gli allegati sospetti [7] anche se provenienti da mittenti conosciuti non devono essere aperti;
3. E' fatto divieto di diffusione incontrollata delle "catene di Sant'Antonio"[8];
4. Utilizzare, nel caso di invio di allegati pesanti, i formati compressi[9];
5. Nel caso in cui si debba inviare un documento all'esterno dell'Ente è preferibile utilizzare un formato protetto da scrittura[10];
6. L'iscrizione a "mailing list" esterne è concessa solo per motivi istituzionali e prima di iscriversi occorre verificare in anticipo se il sito è affidabile;
7. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti;
8. E' obbligatorio controllare i file allegati posta elettronica prima del loro utilizzo[11];

Non è consentito utilizzare abbonamenti Internet privati per collegamenti alla rete.

Articolo VII. Uso della rete Internet e dei relativi servizi.

L'Ente mette a disposizione dei dipendenti l'accesso ad Internet attraverso l'uso di un Proxy Server che, per ridurre il rischio di usi impropri[12] della "navigazione web", consente di adottare opportune misure atte a prevenire controlli successivi sul lavoratore In particolare l'Ente adotta una o più delle seguenti misure:

---

[7] file con estensione .exe .scr .pif .bat .cmd

[8] messaggi a diffusione capillare e moltiplicata

[9] *.zip *.rar *.jpg

[10] ad esempio il formato Acrobat *.pdf

[11] non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti

[12] consistenti in attività non correlate alla prestazione lavorativa quali la visione di siti non pertinenti, l'*upload* o il *download* di *file*, l'uso di servizi di rete con finalità ludiche o estranee all'attività

a. individuazione di categorie di siti considerati correlati o meno con la prestazione lavorativa;
b. configurazione di sistemi ed utilizzo di filtri che prevengano determinate operazioni reputate incoerenti con l'attività lavorativa[13];
c. utilizzo di file di log riferiti al traffico web per la produzione di report statistici con indicazione dei siti visualizzati ed identificazione di utenti con maggiore traffico;
d. conservazione dei dati strettamente limitata al perseguimento di finalità organizzative, produttive e di sicurezza.

L'Ente può effettuare precisi controlli sui file di log e sulle singole postazioni di lavoro dopo averne data informativa al lavoratore almeno 3 giorni prima. Tali controlli, a seconda dei casi, possono determinare il trattamento di informazioni personali, anche non pertinenti o idonei a rivelare convinzioni religiose, filosofiche o di altro genere, opinioni politiche, lo stato di salute o la vita sessuale.

I Dirigenti di settore accordano l'accesso a Internet inviando al responsabile del SI regolare richiesta firmata dal lavoratore che sarà informato delle misure adottate dall'Ente per la navigazione su web.

Il PC abilitato alla navigazione in Internet costituisce uno strumento aziendale 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.

Non possono essere utilizzati modem privati per il collegamento alla rete.

E' fatto divieto all'utente lo scarico di software gratuito e shareware prelevato da siti Internet, se non espressamente utili all'attività istituzionale dell'Ente.

E' fatto divieto di utilizzare software pear to pear (P2P) per lo scarico di qualunque tipo di file[14].

---

[13] l'*upload* , l'accesso a determinati siti, il *download* di *file* o *software* aventi particolari caratteristiche dimensionali o di tipologia di dato

[14] esempio Emule

E' vietata la partecipazione a forum non professionali, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi.

Per l'accesso ad internet dovranno essere utilizzate le credenziali di accesso fornite dall'ufficio SI.

Articolo VIII. Protezione antivirus.

Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo [15]

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

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 senza spegnere il computer segnalare l'accaduto al responsabile del SI.

Ogni dispositivo magnetico 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..

Articolo IX. Non osservanza della normativa aziendale.

Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile, per i dipendenti, con provvedimenti disciplinari previste dalle normative vigenti, dal CCNL e dal regolamento disciplinare dell'Ente per gli amministratori e altro personale saranno applicate le sanzioni civili e penali previste dalle normative vigenti.

[15] ad esempio non aprire mail o relativi allegati sospetti, non navigare su siti non professionali ecc..