COMUNE DI SAN MINIATO

PROVINCIA DI PISA

REGOLAMENTO INTERNO PER L'UTILIZZO DEI SISTEMI INFORMATICI E PER IL TRATTAMENTO DEI DATI PERSONALI

Approvato con Deliberazione Giunta Comunale n. 171 del 12.11.2012.
In vigore dal 01.12.2012.

INDICE

Premessa

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

Premesso quindi che l'utilizzo delle risorse informatiche e telematiche del nostro Ente deve sempre ispirarsi al principio della diligenza e correttezza, è stato adottato un Regolamento interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati.

1. Entrata in vigore del regolamento, pubblicità e campo di applicazione

1.1. Il nuovo regolamento entrerà in vigore a partire dalla data di approvazione e copia dello stesso verrà consegnato, o reso disponibile, a ciascun incaricato.

1.2. Per "incaricato" deve intendersi ogni persona fisica designata tale dal Titolare o Responsabile del trattamento (a titolo esemplificativo si citano: dipendenti, collaboratori, lavoratori somministrati, stagisti, tirocinanti). Tale figura potrà anche venir indicata quale "utente".

2. Utilizzo del personal computer

2.1. Il personal computer affidato all'utente 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.

2.2. L'accesso all'elaboratore è protetto da password che deve essere custodita dall'utente con la massima diligenza e non divulgata.

2.3. Non è consentito installare autonomamente programmi provenienti dall'esterno salvo previa autorizzazione del Responsabile sistemi informativi (o persona/ufficio dallo stesso incaricata), in quanto sussiste il grave pericolo di portare virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore.

2.4. Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dal Responsabile sistemi informativi (o persona/ufficio dallo stesso incaricata). L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'Ente a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software (L. 633/41 e successive modifiche; D.Lgs. 518/92 sulla tutela giuridica del software; L. 248/2000, nuove norme di tutela del diritto d'autore; L. 128/2004 e successive modifiche) che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore.

2.5. Non è consentito all'utente modificare le caratteristiche impostate sul proprio PC, salvo previa autorizzazione esplicita del Responsabile sistemi informativi (o persona/ufficio dallo stesso incaricata).

2.6. 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.

2.7. Non è consentita l'installazione sul proprio PC di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, hd usb, ...), se non con l'autorizzazione espressa del Responsabile sistemi informativi (o persona/ufficio dallo stesso incaricata).

2.8. In caso di assenza dell'utente e per improrogabili esigenze lavorative, il Titolare (o Responsabile) del trattamento può richiedere in forma scritta al Responsabile sistemi informativi, di utilizzare il personal computer dell'utente assente, o di assegnare tale postazione di lavoro ad altro incaricato, al fine di prendere visione delle informazioni/documenti necessari per garantire l'ordinaria operatività dell'Ente. Il Titolare (o Responsabile) del trattamento deve informare quanto prima l'utente dell'avvenuto accesso, fornendo adeguata motivazione.

3. Gestione ed assegnazione delle credenziali di autenticazione

3.1. Le password di ingresso alla rete, di accesso ai programmi e dello screen saver sono previste ed attribuite dal Responsabile sistemi informativi (o persona/ufficio dallo stesso incaricata).

3.2. E' necessario procedere alla modifica della password a cura dell'incaricato del trattamento al primo utilizzo e, successivamente, almeno ogni tre mesi (come previsto dall'art. 5 del disciplinare tecnico allegato al D.Lgs. n. 196/2003, "Codice della privacy").

3.3. Le password possono essere formate da lettere (maiuscole o minuscole) e numeri ricordando che lettere maiuscole e minuscole hanno significati diversi per il sistema; devono essere composte da almeno otto caratteri e non devono contenere riferimenti agevolmente riconducibili all'incaricato.

3.4. La password deve essere immediatamente sostituita, dandone comunicazione al Responsabile sistemi informativi (o persona/ufficio dallo stesso incaricata), nel caso si sospetti che la stessa abbia perso la segretezza.

3.5. Per garantire maggiore sicurezza della password si raccomanda di non utilizzare la stessa parola chiave per sistemi di autenticazione interni alla rete dell'Ente e per sistemi di autenticazione privati ed esterni (esempio l'accesso a web mail o ad altri sistemi web).

3.6. Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia al Responsabile sistemi informativi (o persona/ufficio dallo stesso incaricata).

4. Utilizzo della rete

4.1. 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. Su queste unità vengono svolte regolari attività di controllo, amministrazione e backup.

4.2. Le password d'ingresso alla rete ed ai programmi sono personali e vanno gestite secondo le procedure impartite. È assolutamente proibito entrare nella rete e nei programmi con altri nomi utente.

4.3. Il Responsabile sistemi informativi (o persona/ufficio dallo stesso incaricata) può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericoloso per la sicurezza dei PC.

4.4. 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. È infatti assolutamente da evitare un'archiviazione ridondante.

4.5. È cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni. È 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.

5. Utilizzo di PC portatili

5.1. L'utente è responsabile del PC portatile assegnatogli e deve custodirlo con 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, ecc...), in caso di allontanamento, devono essere custoditi in un luogo protetto.

6. Utilizzo e custodia di supporti rimovibili

6.1. In linea generale, non viene raccomandata la copia su floppy disk, Cd rom, nastri, hd usb o simili (di seguito "supporti rimovibili") di dati sensibili e giudiziari, per ridurre al minimo il rischio di perdita o distruzione anche accidentale dei dati stessi. Ciò premesso, ove nello svolgimento della normale attività assegnata all'incaricato, nell'ambito del suo profilo di autorizzazione, sia indispensabile effettuare una copia di dati sensibili e giudiziari su supporti rimovibili, occorre attenersi alle seguenti cautele:

- accertarsi che il supporto rimovibile sia debitamente formattato e privo di altri file, che potrebbero essere infetti. Nel dubbio, è sempre bene provvedere alla formattazione ex novo prima dell'utilizzo;
- il supporto rimovibile, se possibile, deve essere contrassegnato da un'etichetta, con una indicazione in chiaro od in codice, tale da permettere all'incaricato di riconoscere immediatamente il contenuto del supporto rimovibile in questione;
- il supporto rimovibile contenente dati sensibili e giudiziari deve essere sempre direttamente e personalmente custodito dall'incaricato che ha realizzato la copia;
- in caso di spedizione ad altro incaricato, occorre accertarsi che il destinatario abbia lo stesso profilo di autorizzazione del mittente e che il supporto rimovibile venga spedito in una busta sigillata, intestata personalmente all'incaricato, con controfirma sul lembo di chiusura;
- non si deve spedire un supporto rimovibile contenente dati sensibili e giudiziari ad un destinatario, senza aver prima concordato con il destinatario stesso le modalità e tempi di consegna ed aver stabilito la procedura che permette di confermare l'avvenuta consegna al destinatario del supporto stesso;
- qualora i dati contenuti sul supporto rimovibile non abbiano più ragione di essere, si deve provvedere immediatamente alla formattazione del supporto rimovibile ed alla asportazione dell'etichetta con la indicazione del contenuto od alla sua cancellazione;
- poiché i supporti rimovibili sono particolarmente sensibili ai campi magnetici, per evitare la cancellazione o danneggiamento, anche accidentali, dei dati, il supporto rimovibile non deve mai essere avvicinato ad un campo magnetico (come ad esempio il magnete di un altoparlante) oppure lasciato abbandonato nelle vicinanze di un trasformatore (come quelli utilizzati in alcune lampade da tavolo);
- i supporti rimovibili contenenti dati sensibili e giudiziari non devono essere esposti ad estremi di temperatura e di umidità; in particolare, non devono essere lasciati esposti al sole in un'autovettura chiusa;
- si faccia sempre attenzione a non dimenticare il supporto rimovibile all'interno del computer quando, al termine della copia, si spegne il computer e ci si allontana;
- qualora il contenuto del supporto rimovibile debba essere copiato su un hard disk, od altro strumento elettronico di trattamento, ci si accerti di cancellare il relativo contenuto dal supporto al termine dell'operazione di trattamento;
- se l'operazione è ragionevolmente possibile, si raccomanda vivamente di compilare un registro con l'indicazione numerica, o con altro contrassegno, ove sono riportati tutti i supporti rimovibili contenenti dati sensibili e giudiziari, la loro ubicazione, le modalità di accesso, gli eventuali estremi di consegna ad altro incaricato autorizzato;
- il supporto rimovibile contenente dati sensibili o giudiziari non deve mai essere lasciato abbandonato sul tavolo, ma deve essere immediatamente posto all'interno di una custodia sicura, quando non utilizzato; in funzione della criticità dei dati archiviati, si può andare da un cassetto della scrivania chiuso a chiave, sino ad un armadio blindato od una cassaforte, idonea alla custodia di supporti magnetici.

7. Uso della posta elettronica

7.1. La casella di posta, assegnata dall'Ente all'utente, è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

7.2. È 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 ed esplicita autorizzazione.

7.3. È buona norma evitare 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.

7.4. Il contenuto dei messaggi di posta inviati e ricevuti con mail dell'Ente (anche del tipo nomecognome@ente.it) non deve essere considerato confidenziale o riservato.

7.5. Il Titolare (o Responsabile) del trattamento, o persona da lui incaricata, potrà occasionalmente visionare il contenuto delle mail dell'Ente se questo si renda strettamente necessario per fini di sicurezza informatica o per improrogabili esigenze lavorative.

7.6. È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario, ma di norma per la comunicazione ufficiale è obbligatorio avvalersi degli strumenti tradizionali (pec, fax, posta,...).

7.7. È obbligatorio controllare i file attachments di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

7.8. È vietato inviare catene telematiche (o di Sant'Antonio). Non si devono in alcun caso attivare gli allegati di tali messaggi.

8. Uso della rete internet e dei relativi servizi

8.1. Il PC assegnato al singolo utente ed abilitato alla navigazione in Internet costituisce uno strumento dell'Ente utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa. È quindi assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa. Sono consentite, fuori dall'orario di lavoro, solo le seguenti attività:
- accesso alle webmail personali;
- operazioni o transazioni finanziarie, ivi comprese le operazioni di remote banking, acquisti on line e simili.

8.2. È fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dal Titolare del trattamento (o persona/ufficio dallo stesso incaricata).

8.3. E' vietato lo scaricamento (download) e l'esecuzione online di file musicali, video o multimediali non attinenti l'attività lavorativa.

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

8.5. È 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).

8.6. Gli eventuali controlli sull'utilizzo della rete internet, compiuti dal personale incaricato della sicurezza informatica interna, potranno avvenire mediante analisi dei "file di log". Il controllo sui file di log non è continuativo ma di carattere eccezionale e verrà effettuato solo in presenza di problematiche di sicurezza. L'utilizzo di tali informazioni (file di log) è ispirato ai principi di pertinenza e non eccedenza ed avverrà nel rispetto delle Linee guida del Garante per posta elettronica e internet (G. U. n. 58 del 10 marzo 2007).

9. Protezione antivirus

9.1. Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico interno mediante virus o altro software malefico. In particolare l'utente deve:
- limitare allo stretto necessario lo scambio fra computer di file con estensione: exe, dll, zip, com, bat, chm, cmd, cpl, hlp, hta, inf, lnk, ocx, pif, reg, scr, url, vbs, rar;
- non aprire gli allegati di posta se non si è certi della loro provenienza;
- non cliccare mai un link presente in un messaggio di posta elettronica di provenienza sconosciuta;
- non cliccare mai, durante la navigazione internet, su banner o link pubblicitari non necessari per l'attività lavorativa.

9.2. Ogni anomalia o problematica relativa a virus ed antivirus dovrà essere prontamente segnalata al Responsabile sistemi informativi (o persona/ufficio dallo stesso incaricata). Nel caso il software antivirus rilevi la presenza di un file infetto non bonificato, l'utente dovrà immediatamente sospendere ogni elaborazione in corso - senza spegnere il PC - e segnalare l'accaduto.

10. Utilizzo dei telefoni, fax e fotocopiatrici dell'Ente

10.1. Il telefono dell'Ente affidato all'utente è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, non essendo quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti all'attività lavorativa stessa.

10.2. Qualora venisse assegnato un cellulare all'utente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Al cellulare si applicano le medesime regole sopra previste per l'utilizzo del telefono interno: in particolare è vietato l'utilizzo del telefono cellulare messo a disposizione per inviare o ricevere SMS o MMS di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa.

10.3. L’eventuale uso promiscuo (anche per fini personali) del telefono cellulare è possibile soltanto in presenza di preventiva autorizzazione scritta del Titolare (o Responsabile) del trattamento (o persona/ufficio dallo stesso incaricata).
10.4. È vietato l’utilizzo dei fax interni per fini personali, tanto per spedire quanto per ricevere documentazione, salva diversa esplicita autorizzazione da parte del Titolare (o Responsabile) del trattamento (o persona/ufficio dallo stesso incaricata).
10.5. È vietato l’utilizzo delle fotocopiatrici interne per fini personali, salvo preventiva ed esplicita autorizzazione da parte del Titolare (o Responsabile) del trattamento (o persona/ufficio dallo stesso incaricata).

11. Controllo e custodia di atti e documenti contenenti dati personali

11.1. L’ Ente ha messo a disposizione appositi locali o archivi ad accesso selezionato (di seguito “luogo sicuro”), ove sono di norma custoditi i documenti contenenti dati personali; come regola generale, tali documenti non devono essere asportati da tale luogo sicuro e, ove ciò avvenga, la asportazione deve essere ridotta al minimo tempo necessario per effettuare le operazioni di trattamento.
11.2. Dal luogo sicuro devono essere asportati solo i documenti strettamente necessari per le operazioni di trattamento e non intere pratiche, se ciò non è necessario.
11.3. Al termine delle operazioni di trattamento, i documenti devono essere immediatamente riposti nel luogo sicuro.
11.4. Per tutto il periodo in cui i documenti sono all'esterno del luogo sicuro, l’incaricato non deve mai perderli di vista, adempiendo ad un preciso obbligo di custodia dei documenti stessi.
11.5. L’incaricato deve inoltre controllare che i documenti composti da numerose pagine o più raccoglitori siano sempre completi, verificando sia il numero dei fogli che l’integrità del contenuto rispetto a quanto presente all’atto del prelievo dal luogo sicuro.
11.6. I documenti di cui sopra non devono essere mai lasciati incustoditi sul tavolo durante il giorno.
11.7. Ci si deve in particolare assicurare che un visitatore o terzo (addetto alla manutenzione, addetto alle pulizie, collega non autorizzato) non possa venire a conoscenza dei contenuti dei documenti.
11.8. Si deve limitare al minimo assoluto il numero di fotocopie effettuate.
11.9. Se le fotocopie hanno ad oggetto dati sensibili si deve mantenere una traccia scritta delle copie effettuate e degli incaricati o responsabili cui le copie sono state inviate.
11.10. Si deve adottare una procedura per la consegna delle copie ai destinatari che dia tutte le garanzie di sicurezza, in particolare utilizzando buste di sicurezza sigillate, oppure effettuando la consegna personalmente, in modo da ridurre al minimo la possibilità che soggetti terzi non autorizzati possano prendere visione del contenuto, od addirittura fotocopiarlo all'insaputa del mittente e destinatario.
11.11. Particolare cautela deve essere presa ove i documenti in questione vengano consegnati in originale ad un incaricato o responsabile debitamente autorizzato.
11.12. I documenti contenenti dati sensibili o dati che, per una qualunque ragione, siano stati indicati dal responsabile come meritevoli di particolare attenzione devono, in fase di affidamento, essere custoditi con la maggior diligenza possibile.
11.13. Nel caso la consegna degli originali o delle fotocopie dei documenti avvenga per posta, ci si accerti che il destinatario abbia effettivamente ricevuto i documenti inviati e che essi siano giunti integri, e quindi non manomessi o alterati in fase di trasporto.
11.14. Eventuali fotocopie non riuscite bene debbono essere distrutte in un apposito distruggitore, se disponibile, oppure devono essere distrutte in modo tale da non consentire la ricostruzione del contenuto.
11.15. È tassativamente proibito utilizzare le fotocopie non riuscite, quando contengono dati personali, come carta per appunti.
11.16. È parimenti tassativamente proibito trasportare all'esterno del posto di lavoro fotocopie non riuscite, da utilizzare altrove come carta per appunti.
11.17. Quando i documenti devono essere trasportati all'esterno del luogo di lavoro, l’incaricato deve tenere sempre con se la cartella o la borsa, nella quale i documenti sono contenuti.
11.18. Durante il trasporto la cartella non deve essere mai lasciata incustodita e preferibilmente deve essere tenuta chiusa a chiave o devono essere azionate le serrature a combinazione.
11.19. Si ricorda inoltre che i soggetti ammessi agli archivi cartacei contenenti dati sensibili dopo l’orario di chiusura degli archivi stessi devono essere identificati e registrati.

11.20. È tassativamente proibito discutere, comunicare o comunque trattare dati personali per telefono, se non si è certi che il corrispondente sia un incaricato, il cui profilo di autorizzazione sia tale da potere trattare i dati in questione.

12. Osservanza delle disposizioni in materia di privacy

12.1. È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza, come indicate nella lettera di designazione di incaricato del trattamento dei dati ai sensi del disciplinare tecnico allegato al D.Lgs. n. 196/2003.

13. Non osservanza della normativa

13.1. Le funzioni di verifica della corretta applicazione delle disposizioni contenute nel presente Regolamento sono assegnate al Responsabile sistemi informativi ed ai Responsabili del trattamento di ogni Settore dell'Ente (o persona/ufficio dagli stessi incaricata).

13.2. Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari previsti dal CCNL (o da altro contratto in essere), nonché con le azioni civili e penali previste dalla legge.

14. Aggiornamento e revisione

14.1. Tutti gli incaricati possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Le proposte verranno esaminate dal Titolare (o Responsabile) del trattamento (o persona/ufficio dallo stesso incaricata).