



# **COMUNE DI PONZANO VENETO**

## **PROVINCIA DI TREVISO**

### **MANUALE**

### **PER L'USO DEGLI STRUMENTI INFORMATICI**

**Codice sulla Privacy approvato con D.Lgs. 196/2003**

#### **INDICE**

|   |      |
|---|------|
| PREMESSA  | p. 2 |
| UTILIZZO DEL PERSONAL COMPUTER                      | p. 2 |
| UTILIZZO DELLA RETE                                 | p. 2 |
| GESTIONE DELLE PASSWORD                             | p. 3 |
| UTILIZZO DEI SUPPORTI MAGNETICI                     | p. 3 |
| UTILIZZO PC PORTATILI                               | p.3  |
| USO DELLA POSTA ELETTRONICA                         | p. 3 |
| USO DELLA RETE INTERNET E DEI RELATIVI SERVIZI      | p. 4 |
| OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PRIVACY | p. 4 |
| NON OSSERVANZA DELLA NORMATIVA AZIENDALE            | p. 4 |
| AGGIORNAMENTO E REVISIONE                           | p. 4 |

## PREMESSA

La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete Internet con i 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 dell'Ente deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro, è stato adottato un Manuale interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati.

## UTILIZZO DEL PERSONAL COMPUTER

Il Personal Computer affidato al dipendente 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.

L'accesso all'elaboratore è protetto da una password che deve essere custodita dall'incaricato con la massima diligenza e **non divulgata**. La stessa password deve essere attivata per l'accesso alla rete, 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 del responsabile dei sistemi informatici (Custode delle password).

Il custode delle parole chiave riservate o suo delegato, per l'espletamento delle sue funzioni, ha la facoltà in qualunque momento di accedere ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica interna ed esterna. Il custode delle parole chiave riservate potrà accedere ai dati ed agli strumenti informatici esclusivamente per permettere all'Ente, titolare del trattamento, di accedere ai dati trattati da ogni incaricato con le modalità fissate dal Comune stesso, al solo fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività comunale nei casi in cui si renda indispensabile ed indifferibile l'intervento, ad esempio in caso di prolungata assenza od impedimento dell'incaricato, informando tempestivamente l'incaricato dell'intervento di accesso realizzato.

Non è consentito installare autonomamente programmi provenienti dall'esterno salvo previa autorizzazione esplicita del responsabile dei sistemi informatici o suo delegato, in quanto sussiste il grave pericolo di portare Virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore.

Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dal responsabile dei sistemi informatici dell'Ente o suo delegato. 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 (D. Lgs. 518/92 sulla tutela giuridica del software e L. 248/2000 nuove norme di tutela del diritto d'autore) che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore.

Non è consentito all'utente modificare **le caratteristiche** impostate sul proprio PC, salvo previa autorizzazione esplicita del responsabile dei sistemi informatici o suo delegato.

Il Personal Computer deve essere **spento ogni sera** prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. 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 del responsabile dei sistemi informatici o suo delegato.

Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il responsabile dei sistemi informatici o suo delegato nel caso in cui vengano rilevati virus.

## UTILIZZO DELLA RETE DEL COMUNE DI PONZANO VENETO

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. Si consiglia al responsabile sistemi informatici di prevedere un backup giornaliero su supporto magnetico (cassette, cd) il quale dovrà essere custodito in un apposito armadio chiuso a chiave (o cassaforte). Al 31 dicembre di ogni anno, inoltre, il suddetto responsabile effettuerà un salvataggio completo depositandolo nell'archivio storico.

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

Il responsabile dei sistemi informatici o suo delegato può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.

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.

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.

## **GESTIONE DELLE PASSWORD**

I codici identificativi (ID) e la password di ingresso alla rete, di accesso ai programmi e dello screen saver, sono previsti ed attribuiti dal responsabile dei sistemi informatici o suo delegato. È necessario procedere alla modifica dell'ID e della password a cura del responsabile dei sistemi informatici almeno ogni sei mesi; nel caso di trattamento di dati sensibili e di dati giudiziari la periodicità della variazione deve essere ridotta a tre mesi (come previsto dal punto 5 del disciplinare tecnico allegato al Codice della privacy, d.lgs.vo n.196/2003) con contestuale comunicazione all'incaricato. 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.

Nel caso si sospetti che la password abbia perso la segretezza, l'incaricato dovrà darne comunicazione al Custode della parola chiave che provvederà immediatamente alla sostituzione.

Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia al responsabile dei sistemi informatici o suo delegato.

## **UTILIZZO DEI SUPPORTI MAGNETICI**

Tutti i supporti magnetici riutilizzabili (floppy disk riscrivibili, cassette, memorie esterne) contenenti dati sensibili e giudiziari devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato (vedi quanto previsto nel Documento programmatico sulla sicurezza). Una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione.

I supporti magnetici contenenti dati sensibili e giudiziari (vedi quanto previsto nel Documento programmatico sulla sicurezza) devono essere custoditi in archivi chiusi a chiave.

## **UTILIZZO DI PC PORTATILI**

L'utente è responsabile del PC portatile assegnatogli dal responsabile dei sistemi informatici 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, ecc...), in caso di allontanamento, devono essere custoditi in un luogo protetto.

## **USO DELLA POSTA ELETTRONICA**

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.

È fatto divieto di utilizzare le caselle di posta elettronica aziendale **info@comune.ponzanoveneto.tv.it o personale per l'ufficio di appartenenza** per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list salvo diversa ed esplicita autorizzazione.

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.

Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per l'Ente deve essere visionata od autorizzata dal Responsabile dell'Area di competenza, o in ogni modo è opportuno fare riferimento alle procedure in essere per la corrispondenza ordinaria.

La documentazione elettronica che costituisce per l'Ente "know how" e che, quindi, viene contraddistinta da diciture od avvertenze dirette ad evidenziarne il carattere riservato o segreto non può essere comunicata all'esterno senza preventiva autorizzazione del Responsabile dell'Area di competenza.

È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario. Il messaggio di ricevuta dell'e-mail non ha valore probatorio e quindi di norma per la comunicazione ufficiale è obbligatorio avvalersi degli strumenti tradizionali (fax, posta, ...). Solo il ricorso alla posta elettronica certificata consente l'invio e la ricezione di messaggi ufficiali rilevanti anche all'esterno dell'Ente.

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

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).

È vietato inviare catene telematiche (o di Sant'Antonio). Se si dovessero ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al responsabile dei sistemi informatici o suo delegato. Non si devono in alcun caso attivare gli allegati di tali messaggi.

## **USO DELLA RETE INTERNET E DEI RELATIVI SERVIZI**

Il PC abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa. È assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.

È fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dal responsabile dei sistemi informatici o suo delegato.

È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dal Responsabile dell'Area di competenza e con il rispetto delle normali procedure di acquisto.

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

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).

## **OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PRIVACY**

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.

## **NON OSSERVANZA DELLA NORMATIVA DELL'ENTE**

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.

## **AGGIORNAMENTO E REVISIONE**

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente manuale. Le proposte verranno esaminate dal Responsabile dell'Area di competenza.

Il presente manuale è soggetto a revisione con frequenza annuale.