COMUNE DI SANT'ANGELO MUXARO
Provincia di AGRIGENTO
***

REGOLAMENTO

PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI COMUNALI

Approvato con delibera di G.M. n. 33 del 13.07.2009

NOTA INTRODUTTIVA

Negli ultimi anni l'utilizzo di risorse informatiche (computer, periferiche, software, internet, interconnessione con altri soggetti) da parte del Comune è notevolmente aumentato in quantità e complessità.

In questo senso, viene fortemente sentita dal Comune la necessità di porre in essere adeguati sistemi di controllo sull'utilizzo di tali strumenti da parte dei dipendenti e di sanzionare conseguentemente quegli usi scorretti che, oltre ad esporre il comune a rischi tanto patrimoniali quanto penali, possono di per sé considerarsi contrari ai doveri di diligenza e fedeltà previsti dagli artt. 2104 e 2105 del codice civile e dall'art. 23 del CCNL.

I controlli preventivi e continui sull'uso degli strumenti informatici devono garantire tanto il diritto del Comune di proteggere la propria organizzazione, essendo i computer strumenti di lavoro la cui utilizzazione personale è preclusa, quanto il diritto del lavoratore a non vedere invasa la propria sfera personale, e quindi il diritto alla riservatezza ed alla dignità come sanciti dallo Statuto dei lavoratori e dal D. Lgs. 196/03 sulla tutela dei dati personali.

Tutto ciò avrebbe importanti ricadute in termini di sicurezza, ed è necessario quindi stabilire una serie di regole di comportamento che, nel rispetto della normativa vigente in tema di trattamenti di dati personali e relative misure minime di sicurezza interna e dei sistemi informatici (direttiva n. 2 del 26/05/2009 del Ministro per la Pubblica Amministrazione e l'Innovazione), garantiscano:

1. le misure necessarie a garantire la sicurezza;
2. la disponibilità e l'integrità dei sistemi informatici;
3. l'efficienza ed il corretto utilizzo delle risorse informatiche;
4. la riservatezza delle informazioni e dei dati;
5. il rispetto delle leggi in materia di risorse in informatiche.

Le sotto riportate regole devono essere seguite da tutti gli utenti della rete comunale e cioè, dipendenti che utilizzano il P.C., amministratori, stagisti, tirocinanti, collaboratori, volontari del servizio civile, etc., significando, altresì, che, per quanto non qui previsto, è comunque richiesto un atteggiamento ispirato alla correttezza ed alla buona fede.

Art. 1 – Ufficio Servizi Sistemi Informatici

1.1 E' costituito nell'ambito del Settore dell'Amministrativo e di Vigilanza l'Ufficio Servizi Sistemi Informatici (USSI).

1.2 L'Ufficio Sistemi Servizi Informatici sarà costituito di n. 3 unità, di cui n. 1, nominato dal Sindaco, sarà il Responsabile del Settore Amministrativo e di Vigilanza, con funzioni di Responsabile, e n. 2 componenti, nominati tra i dipendenti comunali con atto del Responsabile del Settore assegnatario del Servizio con l'attribuzione delle relative mansioni, che abbiano maturato esperienza specifica nel campo dell'informatica.

Art. 2 – Utilizzo del Personal Computer

2.1 Il Personal Computer affidato al dipendente è uno strumento di lavoro. Il dipendente affidatario ha l'obbligo, così come sancito da norme di legge e di contratto, di adottare nell'uso dello strumento comportamenti conformi al corretto espletamento della prestazione della propria attività lavorativa ed idonei a non causare danni o pericoli ai beni e/o strumenti ad esso affidati dall'Amministrazione che potrebbero 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'incaricato con la massima diligenza e non divulgata. Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte del Responsabile del Settore assegnatario del Servizio dei Sistemi Informatici.

2.3 Il Responsabile del Settore assegnatario del Servizio dei Sistemi Informatici (di seguito RSSI) per l'espletamento delle funzioni e mansioni assegnate, ha la facoltà in qualunque momento di accedere ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica, anche delegando a terzi con specifico informale mandato, in relazione agli scopi di volta in volta identificati.

2.4 Non è consentito installare autonomamente programmi provenienti dall'esterno senza la preventiva autorizzazione del RSSI ed una richiesta scritta da parte del Responsabile del Settore dell'unità cui è assegnato il P.C..

2.5 Non è consentito l'uso di programmi diversi da quelli distribuiti ufficialmente dal Servizio Sistemi Informativi del Comune di Sant'Angelo Muxaro (d. lg. 518/92 sulla tutela giuridica del software e L. 248/2000 nuove norme di tutela del diritto d'autore).

2.6 Non è consentito all'utente modificare le caratteristiche impostate sui P.C. assegnati, i punti rete di accesso e le configurazioni delle reti LAN/WAN presenti nelle sedi, salvo autorizzazione esplicita del Responsabile del Servizio Sistemi Informativi.

2.7 E' responsabilità del Responsabile dei Servizi Sistemi Informatici verificare il coerente utilizzo delle risorse assegnate ed evitarne l'uso improprio o l'accesso alle risorse da parte di personale non autorizzato, compreso l'utilizzo da parte di terzi di punti rete in luoghi non presidiati.

2.8 Il Personal Computer deve essere spento al termine delle attività lavorative o in caso di assenze prolungate dall'ufficio. In ogni caso deve essere attivato lo screen saver e la relativa password.

2.9 Il dipendente ha l'obbligo di impedire ad altri indebiti utilizzi della propria apparecchiatura informatica non avendo rilevanza al fine del difetto di responsabilità, nell'impossibilità di provarne in seguito l'indebito uso, il fatto che altri, in sua assenza, abbia potuto usare la postazione lavorativa. In difetto, il comportamento del dipendente si configura come negligente, inescusabile e gravemente colposo.

2.10 Non è consentita l'installazione sul proprio P.C. o il collegamento sulla rete LAN di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, P.C. portatili ed apparati in genere …), se non con l'autorizzazione espressa dal Responsabile del Servizio Sistemi Informatici, previa richiesta scritta da parte del Responsabile del Settore dell'unità cui è assegnato il P.C..

2.11 E' fatto, altresì, obbligo di distruggere eventuali copie di sicurezza o supporti di tipo removibile (floppy, CD-Rom, Nastri) una volta non sia possibile rendere irrecuperabili i dati in essi contenuti.

2.12 Ai sensi del D. Lgs n. 196/03 è fatto divieto di divulgazione a qualsiasi titolo delle informazioni presenti nelle banche dati dell'ente se non disciplinate da appositi protocolli di intesa.

2.13 Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il RSSI nel caso in cui siano rilevati virus ed adottando quanto previsto dal successivo punto 7 del presente Regolamento relativo alle procedure di protezione antivirus.

2.14 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.

2.15 E' prevista la progressiva erogazione di tutti servizi di supporto (Help Desk) per le problematiche funzionali di tipo hardware e software, attraverso procedure informatiche centralizzate.

Art. 3 – Utilizzo della rete LAN

3.1 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, potranno essere svolte regolari attività di controllo, amministrazione e backup da parte dell'Amministratore del Sistema. Al fine di garantire la corretta gestione delle politiche di sicurezza delle informazioni è fatto divieto di replicare su dischi locali dei P.C. dati, banche dati e documenti sensibili senza esplicita autorizzazione del RSSI e senza l'adozione di adeguate politiche di sicurezza, quali la crittazione dei dati stessi e l'adozione di politiche di backup comprensive della dotazione di idonei archivi protetti.

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

3.3 Il RSSI può in qualunque momento procedere, previa informazione/consultazione delle rappresentanze provinciali dei lavoratori previste dai contratti collettivi, alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui P.C. degli incaricati sia sulle unità di rete.

3.4 Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con la cancellazione dei file obsoleti o inutili, riducendo l'eventuale conservazione nel tempo dei dati limitatamente al perseguimento delle finalità organizzative, produttive e di sicurezza. Particolare attenzione deve essere prestata alla duplicazione dei dati. E' infatti assolutamente da evitare un'archiviazione ridondante.

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

3.6 Non è consentito collegare reti di P.C. od altri dispositivi alla rete aziendale senza la preventiva autorizzazione scritta dell'Amministratore di Sistema ed una verifica della conformità agli standard tecnici presenti.

Art. 4 – Gestione delle Password

4.1 Ad ogni utente sono assegnate delle credenziali personali di accesso al computer ed al dominio di rete formate da un nome utente e da una password: il nome utente è formato dal cognome seguito dal nome; la password inizialmente fornita sarà costituita dalla data di nascita dell'utente che verrà cambiata con altra, liberamente scelta dallo stesso, nel rispetto della privacy di ciascuno, in presenza del Responsabile dei Servizi Sistemi Informatici abilitato al quale l'utente dovrà consegnarla, in busta chiusa e sigillata, per essere conservata agli atti del Comune in posto sicuro e certo. L'utente può cambiarla in qualsiasi momento facendone richiesta al RSSI. La password soggiace ai criteri di complessità previsti dalla normativa vigente (numero di caratteri, scadenza, ecc.), e deve essere mantenuta riservata: non ci sono ragioni tecniche che giustifichino la condivisione delle proprie credenziali di accesso con altri utenti;

4.2 Le credenziali di accesso di ciascun dipendente inquadrato in una determinata U.O. permettono:

- l'accesso a tutti i P.C. di quella Unità Organizzativa, e l'utilizzo di qualsiasi risorsa locale (files sul disco fisso, stampanti, programmi, posta elettronica);
- l'accesso alle risorse di rete assegnate all'ufficio o specifiche di quell'utente (cartella "condivise" sul server, stampanti di rete ecc.);
- l'accesso ad internet;

4.3 se necessario per ragioni di manutenzione, il RSSI può cambiare la PW in presenza dell'interessato secondo le modalità riportate al punto 4.1;

4.4 Durante le sessioni di lavoro i P.C. non possono essere lasciati incustoditi ed accessibili a terzi. Pertanto ogni qualvolta l'utente si allontani o si assenti dalla postazione è tenuto a bloccarne l'accesso o chiudere la sessione e disconnettere il proprio utente.

4.5 La password deve essere immediatamente sostituita, dandone comunicazione al RSSI, nel caso si sospetti che la stessa abbia perso la segretezza.

4.6 Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia al RSSI.

4.7 E' dato incarico ai Responsabili di Settore di comunicare tempestivamente eventuali cambi di mansione che comportino modifiche o revoche di autorizzazione all'accesso delle risorse informatiche, sia all'ufficio del personale che al Responsabile dei sistemi informatici, per

iscritto, al fine di rendere possibili le modifiche dei profili di accesso alle risorse e la sostituzione delle password ove necessario.

4.8 Tutti i nomi utenti e le password di eventuali collegamenti istituzionali esterni al comune devono rispettare le sopra riportate regole.

Art. 5 – Utilizzo dei supporti magnetici

5.1 Tutti i supporti magnetici riutilizzabili contenenti dati sensibili devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato. Una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione.

5.2 I supporti magnetici contenenti dati sensibili e le copie di backup devono essere custoditi in archivi chiusi a chiave in buste contenente: Ufficio, responsabile di backup, data di archiviazione.

5.3 Non è consentito scaricare files contenuti in supporti magnetici/ottici non aventi alcuna attinenza con la propria prestazione lavorativa.

5.4 Tutti i files di provenienza incerta, ancorché potenzialmente attinenti all'attività lavorativa, non devono essere utilizzati/installati/testati. Nel caso di effettiva necessità di impiego devono essere sottoposti ad un preventivo controllo ed alla relativa autorizzazione all'utilizzo da parte del RSSI.

Art. 6 – Uso della posta elettronica

6.1 La casella di posta, assegnata all'utente, è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse. Si rammenta che i sistemi di posta elettronica non consentono al momento di garantire la riservatezza delle informazioni trasmesse, si raccomandano gli utenti di non inoltrare dati ed informazioni classificabili "sensibili" o "riservate" con questo mezzo.

6.2 E' fatto divieto di utilizzare le caselle di posta elettronica ……@comunedisantangelo muxaro.it per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list non attinenti la propria attività o funzione svolta per l'ente, salvo diversa ed esplicita autorizzazione.

6.3 E' 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.

6.4 Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per il Comune di Sant'Angelo Muxaro ovvero contenga documenti da considerarsi riservati in quanto contraddistinti dalla dicitura "strettamente riservati" o da analoga dicitura, deve essere visionata od autorizzata dal Responsabile cui si riferisce l'attività.

6.5 Per la trasmissione di file all'interno del Comune di Sant'Angelo Muxaro è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati, se di dimensioni consistenti si consiglia di utilizzare le directory di scambio presenti sui file server, notificando a mezzo mail al destinatario la disponibilità del file stesso.

6.6 E' obbligatorio controllare con il Sw antivirus 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).

6.7 Per rendere maggiormente evidente anche all'esterno la natura non personale dell'utilizzo delle mail assegnate agli uffici del comune è obbligo inserire alla fine di ogni messaggio mail spedito la seguente dicitura: "L'indirizzo xxx@comunedisantangelomuxaro.it si riferisce ad una casella di posta elettronica istituzionale assegnata all'ufficio xxxx del Comune di Sant'Angelo Muxaro; le comunicazioni inviate a tale indirizzo sono conoscibili da tutti gli appartenenti a tale ufficio e, se giuridicamente rilevanti, verranno registrate nel protocollo ufficiale del Comune.

Art. 7 – Uso della rete Internet e dei relativi servizi

7.1 Il P.C. abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa. E' proibita la navigazione in Internet per motivi diversi da quelli funzionali all'attività lavorativa stessa.

7.2 La navigazione in internet a fini personali utilizzando i P.C. dell'ufficio è vietata. Per navigazione a fini personali si intende a titolo esemplificativo e non esaustivo:

- l'utilizzo della propria mail tramite sistemi di web-mail o con la configurazione di programmi di posta;
- l'effettuazione di pagamenti ed acquisti on-line, la consultazione di cataloghi di beni o servizi per acquisti privati;
- l'accesso a corsi di studio on line, o la ricerca e consultazione di materiale di studio per corsi tradizionali frequentati a scopi personali;
- l'accesso a siti di giornali on line, agenzie di stampa, blog e a siti informativi in generale per motivi non attinenti alle mansioni da espletare;

7.3 E' fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato dai siti Internet, se non espressamente autorizzato dal RSSI.

7.4 E' 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 o attinenti i compiti e le mansioni assegnate e con il rispetto delle normali procedure di acquisto.

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

7.6 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), se non attinenti l'attività lavorativa svolta.

7.7 Il Responsabile dei Servizi Sistemi Informatici si riserva di applicare per singoli e gruppi di utenti politiche di navigazione personalizzate in base alle mansioni ed eventuali disposizioni concordate con l'Amministrazione e con i Responsabili dei Settori, al fine di ottimizzare l'uso delle risorse, gli investimenti e le prestazioni delle connessioni esistenti.

7.8 Non è consentito visitare siti dai contenuti di natura oltraggiosa e/o discriminatoria per sesso/etnia/religione/opinione e/o appartenenza sindacale e/o politica quali, a titolo esemplificativo:

- pornografia;
- gioco d'azzardo on-line;

- violenza istigazione all'odio, armi;
- attivismo politico, religiosità, spiritualità.

7.9 I dati relativi alla navigazione in internet dai P.C. della rete comunale (nello specifico: nome utente - Data della connessione – Ora della connessione – Indirizzo di rete del P.C. comunale – servizio richiesto dal P.C. comunale [es. web, mail, ftp ecc.] – Indirizzo di rete computer chiamato [server o generalmente host] [es. server web, mail ecc.] – Esito della richiesta [operazione permessa/bloccata] – riferimento alla regola del firewall) sono memorizzati tramite i dispositivi sopra citati e possono essere oggetto di controllo.

art. 8 – Protezione antivirus

8.1 Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo.
8.2 Ogni utente è tenuto a controllare il regolare funzionamento e l'aggiornamento periodico del software antivirus installato, secondo le procedure previste.
8.3 Nel caso che il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente:

a) sospendere ogni elaborazione in corso senza spegnere il computer
b) segnalare l'accaduto al Responsabile del Servizio Sistemi Informativi.

8.4 Non è consentito l'utilizzo di floppy disk, cd rom, cd riscrivibili, nastri magnetici di provenienza ignota.
8.5 Ogni dispositivo magnetico di provenienza esterna dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere consegnato al responsabile dei sistemi informativi.

Art. 9 – l Controlli

9.1 Controlli Internet:

A. Viene garantito al Responsabile dei servizi dei sistemi informativi l'accesso ai dati memorizzati dai dispositivi di sicurezza. L'accesso ai dati è graduato in modo da considerarli in prima analisi in forma complessiva ed anonima, cioè non direttamente riconducibili ad un utente:

B. il traffico internet complessivo diviso per fascia oraria con quantificazione degli eventi e della quantità di dati scambiati;

C. La rilevazione di anomalie quali ad esempio a titolo meramente esemplificativo:

- l'utilizzo di internet in orario non compatibile con gli orari di servizio;

- la consultazione di siti ritenuti non attinenti con l'attività lavorativa, in relazione al loro contenuto, o perché la modalità o frequenza di consultazione lasci presumere un utilizzo a fini personali;

D. l'utilizzo ritenuto eccessivo dei servizi internet e di mail può dar luogo:

- ad un richiamo collettivo al rispetto delle regole previste nel presente regolamento;
- in caso di reiterazione dei comportamenti ritenuti scorretti, alla loro precisazione e quantificazione, alla identificazione del soggetto che li compie, ed all'attivazione delle conseguenti sanzioni disciplinari;

9.2 Controlli sull'utilizzo delle mail istituzionali:

A. Viene garantita al RSSI la possibilità di accedere con le proprie credenziali a tutti i P.C. e di conseguenza la possibilità di accedere alle mail e rilevare eventuali utilizzi impropri. Tale controllo viene svolto, previa informazione/consultazione delle rappresentanze provinciali dei lavoratori previste dai contratti collettivi, alla presenza del dipendente o dei dipendenti utilizzatori del P.C. senza ulteriori formalità.

9.3 Controlli sui P.C. degli utenti:

A. Viene garantito al RSSI, previa informazione/consultazione delle rappresentanze provinciali dei lavoratori previste dai contratti collettivi, l'accesso alle cartelle di ogni ufficio memorizzate sul server ed ai dischi fissi dei singoli P.C. direttamente dalla propria postazione. Qualora risultasse una violazione rispetto a quanto stabilito all'art. 9, procederà alla copia del materiale ritenuto non conforme al presente regolamento, all'identificazione del soggetto autore dell'abuso ed all'attivazione delle conseguenti sanzioni disciplinari.

B. Nell'esercizio del potere di controllo l'Amministrazione deve, comunque, ispirare il proprio comportamento al rispetto del principio di proporzionalità, che si concreta nella pertinenza e non eccedenza delle attività di controllo (le limitazioni della libertà e dei diritti individuali devono essere proporzionate alla scopo perseguito). E' esclusa, in ogni caso, l'ammissibilità di controlli prolungati, costanti e indiscriminati.

Art. 10 – Osservanza delle disposizioni in materia di Privacy

10.1 E' obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza. Tale norma andrà indicata nelle lettere di individuazione dell'incaricato al trattamento dei dati ai sensi del D. Lgs. n. 196/03.

Art. 11 – Non osservanza della normativa

11.1 Il mancato rispetto o la violazione delle regole contenute nel presente Regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

11.2 I lavoratori devono, comunque, essere preventivamente informati dell'esistenza di dispostivi di controllo atti a raccogliere dati personali.

11.3 Al fine di assicurarne la massima pubblicità, il presente Regolamento sarà pubblicato mediante affissione in luogo accessibile a tutti e, più in generale, nel rispetto delle procedure previste dall'art. 7 dello Statuto dei Lavoratori.

Art. 12 – Aggiornamento e revisione

11.1 Tutti gli utenti possono proporre, modifiche o integrazioni al presente Regolamento nel rispetto delle normative .