COMUNE DI SAN STINO DI LIVENZA
Provincia di Venezia

Regolamento per l’utilizzo degli strumenti informatici e telematici

INDICE ANALITICO

PREMESSA

La progressiva diffusione delle tecnologie informatiche, ed in particolare il libero accesso alla rete internet dai personal computer, di cui sono dotate le postazioni di lavoro negli uffici comunali, espone il Comune di San Stino di Livenza a rischi connessi alla sicurezza del sistema informativo ed alla riservatezza delle informazioni con possibili conseguenze e coinvolgimenti di tipo patrimoniale e penale.
Le disposizioni emanate dall'Autorità Garante, mediante il provvedimento di carattere generale (Del. N. 13 dell'1.3.2007) in cui vengono definite le linee guida per l'utilizzo della posta elettronica ed internet, nonché la più recente Direttiva N. 2 del 26 maggio 2009 del Ministro per la Pubblica Amministrazione e l'Innovazione con la quale si evidenziano i doveri dei dipendenti pubblici nell'utilizzo degli strumenti informatici e le regole per l'esercizio del potere di controllo da parte delle Amministrazioni, impongono l'adozione di precise e definite regole per l'utilizzo di tali strumenti.
Le prescrizioni che seguono sono formulate in attuazione del D. Lgs. n. 196/2003 e successive modifiche ed integrazioni, sulle misure di sicurezza obbligatorie ed in conformità a quanto evidenziato nel provvedimento dell'Autorità Garante appena citato, tenuto conto che:

- l'utilizzo delle risorse informatiche e telematiche del Comune di San Stino di Livenza deve avvenire sempre con diligenza e correttezza e l'adozione di un regolamento interno è diretto ad evitare che comportamenti, anche inconsapevoli, possano innescare problemi o minacce alla sicurezza nel trattamento dei dati e pregiudicare od ostacolare le attività dell'Amministrazione, o, addirittura, perseguire interessi privati in luogo od in contrasto con quelli pubblici;
- compete al datore di lavoro assicurare la funzionalità ed il corretto impiego di tali mezzi da parte dei lavoratori, definendone le modalità d'uso nell'organizzazione dell'attività lavorativa, tenendo conto della disciplina in termini di diritto del lavoro;

Art. 1 - UTILIZZO DEL PERSONAL COMPUTER

1. Il personal computer (in avanti, per brevità, PC) affidato a ciascun dipendente o a chiunque, comunque, lo utilizzi a vario titolo, è da considerare uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza, e pertanto il PC non deve essere usato per attività non inerenti al rapporto lavorativo salvo quanto previsto al comma 7 dell'articolo 7.
2. L'accesso al PC è protetto da password che deve essere gestita con le modalità definite dal documento programmatico per la sicurezza vigente (riepilogate al successivo articolo 3), custodita dall'incaricato con la massima diligenza e non divulgata se non, in caso di temporanea necessità, al responsabile della sicurezza, amministratore del sistema (in avanti, per brevità, sarà riportato amministratore del sistema). La password deve essere attivata per l'accesso alla rete, per l'accesso a qualsiasi applicazione, per lo screen saver. Non è consentita l'attivazione della password di accensione (bios).
3. L'amministratore del sistema, per l'espletamento delle sue funzioni e per esigenze organizzative (ad es. per rilevare anomalie o per manutenzioni del sistema) o connesse alla sicurezza dell'attività lavorativa, può avvalersi, nel rispetto dello Statuto del Lavoratori (art. 4, comma 2), di sistemi che consentono indirettamente un controllo a distanza (c.d. controllo preterintenzionale) e che determinano un trattamento di dati riferiti o riferibili ai lavoratori. Tale trattamento sarà operato nel rispetto delle procedure di informazione e consultazione dei lavoratori.
4. Non è consentito installare autonomamente programmi, salvo espressa autorizzazione dell'amministratore del sistema, in quanto sussiste il grave pericolo di introdurre virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore e di conseguenza dell'intero sistema in rete. Inoltre non è consentito l'uso di programmi diversi da quelli distribuiti ufficialmente dal Comune di San Stino di Livenza (D. Lgs. n. 518/92 sulla tutela giuridica del software e L. n. 248/2000 sulla tutela del diritto d'autore).
5. Non è consentito all'utente modificare le caratteristiche impostate sul proprio PC, salvo espressa autorizzazione dell'amministratore del sistema.

6. Il PC deve essere spento ogni sera prima di lasciare gli uffici e in caso di allontanamento dalla propria postazione di lavoro, deve essere attivato lo screen saver protetto da password, onde impedirne l'indebito uso da parte di terzi.

7. Non è consentita l'installazione sul proprio PC di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, ecc.), se non con l'autorizzazione dell'amministratore del sistema.

8. Ai dipendenti incaricati del trattamento dei dati sensibili è fatto divieto l'accesso contemporaneo con lo stesso account da più PC.

9. Chiunque utilizzi i PC deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente l'amministratore del sistema nel caso in cui siano rilevati virus ed adottando quanto previsto dal successivo articolo 8 del presente regolamento relativo alle procedure di protezione antivirus.

10. 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, politica e/o filosofica.

Art. 2 - UTILIZZO DELLA RETE INFORMATICA DEL COMUNE

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. Sulle stesse, vengono svolte regolari attività di controllo, amministrazione e backup da parte dell'amministratore del sistema, e dagli incaricati anche esterni e temporanei individuati per funzioni specifiche.

2. L'amministratore del sistema, può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza e la funzionalità sia dei singoli PC degli incaricati che delle unità di rete condivise.

3. Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutilizzati.

Art. 3 - GESTIONE DELLE PASSWORD

1. Le password di ingresso alla rete, di accesso ai programmi e dello screen saver, sono previste ed attribuite inizialmente dall'amministratore del sistema. E’ obbligatoria al primo utilizzo l'autonoma sostituzione della password da parte del/i dipendente/i. L’amministratore del sistema, dopo l’autonoma sostituzione della password da parte del dipendente, non sarà più a conoscenza di questa, ma ha facoltà di resettarla per motivi di servizio. In caso di cancellazione della password, l’amministratore del sistema comunicherà la cancellazione della medesima al dipendente interessato, che provvederà a una nuova autonoma obbligatoria sostituzione, prima di iniziare a utilizzare la postazione a sua disposizione.

2. La password, quando e' prevista dal sistema di autenticazione, e' composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito. Essa non deve contenere riferimenti agevolmente riconducibili al dipendente (non solo nomi, cognomi, soprannomi, ma neppure date di nascita, proprie, dei figli o degli amici), né consistere in nomi noti, anche di fantasia (pippo, pluto, etc.). La password è modificata obbligatoriamente dal dipendente incaricato al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave deve essere modificata almeno ogni tre mesi.

Art. 4 - UTILIZZO DEI SUPPORTI DI MEMORIZZAZIONE REMOVIBILI

1. I supporti removibili non devono contenere dati sensibili o giudiziari. I supporti removibili, se non utilizzati, sono distrutti o resi inutilizzabili.

2. Non è consentito scaricare file contenuti in supporti removibili non aventi alcuna attinenza con la propria attività lavorativa.

3. Ogni dispositivo magnetico di provenienza esterna al Comune di San Stino di Livenza dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere fatta segnalazione all'amministratore del sistema.

Art. 5 - UTILIZZO DI PC PORTATILI

1. Il dipendente è responsabile del PC portatile assegnatogli anche temporaneamente e deve custodirlo con estrema diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

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.

3. I PC portatili utilizzati all'esterno (convegni, incontri, meeting ecc.), in caso di allontanamento, devono essere custoditi in un luogo protetto.

Art. 6 - USO DELLA POSTA ELETTRONICA

1. La casella di posta elettronica, assegnata dal Comune di San Stino di Livenza al dipendente, o ad altra figura all'interno dell'amministrazione, è uno strumento di lavoro. Gli assegnatari delle caselle di posta elettronica sono responsabili personalmente del contenuto e del corretto utilizzo delle stesse.

2. E' fatto divieto di utilizzare le caselle di posta elettronica del Comune di San Stino di Livenza, per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mailing-list non attinenti all'attività lavorativa.

3. E' fatto divieto di inviare e/o ricevere 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.

4. E' possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario, ma per la comunicazione ufficiale è obbligatorio avvalersi degli strumenti tradizionali (fax, posta) a meno che la comunicazione non avvenga tramite PEC Posta Elettronica Certificata.

5. E' obbligatorio controllare i file allegati ai messaggi di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

6. E' vietato partecipare a catene telematiche (o di Sant'Antonio). Se si dovessero ricevere messaggi di tale tipo, deve essere comunicato immediatamente all'amministratore del sistema. Non si deve in alcun caso attivare gli allegati di tali messaggi.

7. Qualora dovesse rendersi necessario conoscere il contenuto dei messaggi di posta elettronica in caso di assenza prolungata od improvvisa e/o per improrogabili necessità legate all'attività lavorativa, l'incaricato dovrà individuare un proprio collega "fiduciario" il quale provvederà a verificare il contenuto dei messaggi e ad inoltrare al responsabile della sicurezza quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Di tale attività sarà redatto un verbale ed informato tempestivamente alla prima occasione utile il lavoratore interessato.

8. Si evidenzia che, qualora dovessero rendersi necessari dei controlli sull'uso degli strumenti elettronici da parte dei lavoratori saranno rispettati i principi di pertinenza e non eccedenza e saranno evitate ingiustificate interferenze sui diritti e sulle libertà fondamentali dei lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata. In tal senso eventuali esigenze connesse ad azioni mirate di controllo saranno effettuate in maniera graduale, riguardando in prima istanza dati aggregati, riferiti all'intera struttura lavorativa o sue specifiche aree, richiamando le stesse ad utilizzo pertinente degli strumenti informatici posti a loro disposizione. Qualora gli esiti dovessero generare l'assenza di successive anomalie saranno effettuati controlli di carattere generale. Si precisa altresì che tali controlli non saranno effettuati in maniera prolungata, costante o indiscriminata, ma mirati ad individuare eventi dannosi o situazioni di pericolo per le quali non sia stato possibile impedirne gli effetti attraverso preventivi accorgimenti tecnici.

Art. 7 - USO DELLA RETE INTERNET E DEI RELATIVI SERVIZI

1. Il PC abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa.
2. E' vietata la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa. A maggior ragione non è consentito navigare in siti che accolgono contenuti contrari alla morale e alle prescrizioni di legge. Non è inoltre consentito navigare in siti che possano rilevare la profilazione dell'individuo definita "sensibile" ai sensi del D. Lgs. n. 196/2003, quindi siti la cui navigazione palesi elementi attinenti alla fede religiosa, alle opinioni politiche, filosofiche e sindacali del dipendente o le sue abitudini sessuali.
3. E' fatto divieto al dipendente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dall'amministratore del sistema.
4. Non è consentito lo scarico di materiale elettronico tutelato dalla normativa sul diritto d'autore (software, file audio, film, etc.) né attraverso Internet, né attraverso servizi peer-to-peer.
5. E' vietata la partecipazione a Forum non professionali, l'utilizzo di chat (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest book anche utilizzando pseudonimi (o nickname).
6. 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.
7. E' regolamentato e, quindi, consentito effettuare adempimenti on line nei confronti di pubbliche amministrazioni e di concessionari di servizi pubblici, ovvero per tenere rapporti con istituti bancari ed assicurativi. Tali attività, pur non rientrando tra i compiti istituzionali, devono essere finalizzate ad assolvere incombenze amministrative e burocratiche senza allontanarsi dal luogo di lavoro e vanno contenute nei tempi strettamente necessari allo svolgimento delle transazioni.
8. E' da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa, salvo quelli eventualmente rientranti nelle situazioni di cui al comma precedente.
9. Si evidenzia che, qualora dovessero rendersi necessari dei controlli sull'uso di Internet da parte dei lavoratori, saranno rispettati i principi di pertinenza e non eccedenza e saranno evitate ingiustificate interferenze sui diritti e sulle libertà fondamentali dei lavoratori. In tal senso eventuali esigenze connesse ad azioni mirate di controllo saranno effettuate in maniera graduale, riguardando in prima istanza dati aggregati, riferiti all'intera struttura lavorativa o gruppi sufficientemente ampi di lavoratori tali da precludere l'immediata identificazione degli utenti (ad es., con riguardo ai *file* di *log* riferiti al traffico). Si precisa altresì che tali controlli non saranno effettuati in maniera prolungata, costante o indiscriminata, ma saranno mirati ad individuare eventi dannosi o situazioni di pericolo per le quali non sia stato possibile impedirne gli effetti attraverso preventivi accorgimenti tecnici. In tal senso il Comune di San Stino di Livenza provvederà ad individuare ed installare dei software (detti comunemente web filter) che prevengano determinate operazioni, reputate inconferenti con l'attività lavorativa, quali l'upload o l'accesso a determinati siti (inseriti in una sorta di black list) e/o il download di file o software aventi particolari caratteristiche (dimensionali o di tipologia di dato).
10. La conservazione dei dati riguardanti l'attività di navigazione internet è regolata in modo che venga automaticamente effettuata la sovraregistrazione dei file, e vengano in tal maniera cancellati periodicamente i dati personali la cui conservazione non sia necessaria. Un eventuale prolungamento dei tempi di conservazione va valutato come eccezionale e può aver luogo solo in relazione:

- ad esigenze tecniche o di sicurezza del tutto particolari;
- all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
- all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

Art. 8 - PROTEZIONE ANTIVIRUS

1. Ogni utilizzatore di PC deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo.

2. Ogni utilizzatore di PC è tenuto a controllare il regolare funzionamento del software installato, segnalandone immediatamente il cattivo funzionamento all'amministratore del sistema.

3. Nel caso che il software antivirus rilevi la presenza di un virus, il dipendente dovrà immediatamente:

a) sospendere ogni elaborazione in corso senza spegnere il computer;
b) interrompere immediatamente il traffico di rete ed internet;
c) segnalare l'accaduto all'amministratore del sistema.

Art. 9 - OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PRIVACY

1. E' obbligatorio attenersi alle disposizioni in materia di privacy e di misure minime di sicurezza, come indicate nella lettera di individuazione di incaricato del trattamento dei dati ai sensi del D. Lgs. n. 196/2003. Il presente regolamento integra il documento programmatico della sicurezza (DPS) vigente adottato dal Comune di San Stino di Livenza.

Art. 10 - NON OSSERVANZA DEL REGOLAMENTO INFORMATICO

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 dalla legge che il Comune di San Stino di Livenza riterrà di avviare.