COMUNE DI PONTEDERA

Provincia di Pisa

REGOLAMENTO PER L' UTILIZZO DELLE RISORSE INFORMATICHE E TELEMATICHE

Art. 1 – Oggetto

Il presente regolamento disciplina le condizioni per il corretto utilizzo degli strumenti informatici, l'uso della posta elettronica e la navigazione in internet ai sensi del codice dell'amministrazione digitale, approvato con D. Lgs. 82/2005 e ss. mm. ii.
Il regolamento fornisce pertanto i parametri per disciplinare compiutamente e a norma di legge l'innovazione nella pubblica amministrazione.

Art. 2 - Modalità di assegnazione, utilizzo, restituzione del personal computer

2.1 - Ogni Personal Computer è sotto la responsabilità dell' ufficio Sistema Informativo ed Innovazione(SII) e in quanto tale quest'ultimo si occupa dell'acquisto e, dopo la configurazione iniziale, dell'installazione e della gestione dello stesso presso gli utenti.
Il SII fornisce l'apparecchiatura ai singoli utenti e, al momento della cessazione del rapporto lavorativo con il Comune di Pontedera, la recupera, controlla che sia nelle stesse condizioni in cui era al momento della consegna, salvo l'usura dovuta al suo corretto utilizzo, e la riconfigura per un utente successivo.
2.2 - L'accesso all'elaboratore è protetto da password per la cui disciplina si rimanda all'articolo 4 del presente regolamento.
2.3 - Non è consentito installare autonomamente programmi di qualunque tipo. Nel caso vi sia la richiesta scritta da parte del Dirigente Responsabile del Settore cui è stato fornito il PC, il personale del SII, verificata la compatibilità dello stesso con gli altri programmi software in uso all'ente e la disponibilità della licenza, provvederà ad installarlo;
2.4 - E' responsabilità del dirigente 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.
2.5 - Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici. In caso di assenze dall'ufficio l'elaboratore, se non viene spento, deve essere lasciato disconnesso oppure deve essere attivato lo screen saver con password abilitata.
2.6 - Non è consentito collegare direttamente sul proprio PC o mediante rete LAN alcun dispositivo di memorizzazione, comunicazione o altro (masterizzatori, modem, pc portatili ed apparati in genere), se non previa approvazione scritta da parte del SII.
2.7 - Per quanto riguarda il trattamento dei dati sensibili, vengono individuati dei profili di autorizzazione per ciascun utente incaricato o per classi omogenee di utenti incaricati, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento. Periodicamente, e comunque almeno annualmente, verrà verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione, secondo quanto previsto ai punti 12,13,14 del disciplinare tecnico in materia di misure minime di sicurezza (allegato B al Dlgs 196/03) e dal documento programmatico sulla sicurezza adottato con delibera di giunta comunale n. 296 del 10/11/05.
2.8 - Ogni utente relativamente ai supporti di memorizzazione dati di terze parti (CD, floppy, chiavi USB), deve rispettare quanto previsto dal successivo art. 9 del presente Regolamento relativo alle procedure di protezione antivirus.
2.9 - Non è consentita la compilazione, ricerca, diffusione e memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.
2.10 - Le anomalie vanno segnalate nella modalità descritta al successivo punto2.11 all' ufficio SII che provvederà al ripristino.

2.11 – Le segnalazioni devono essere effettuate in via prioritaria utilizzando il sistema on line “Sysaid” altrimenti inviando un messaggio di posta elettronica all' indirizzo: assistenza@comune.pontedera.pi.it altrimenti portando richiesta scritta all' ufficio SII. E' prevista l’erogazione di tutti i servizi di supporto (Help Desk) per le problematiche funzionali di tipo hardware e software, attraverso procedure informatiche centralizzate.

Art. 3 - Utilizzo della rete del Comune di Pontedera

3.1 - Le risorse di rete che trasferiscono i dati dell’ente devono essere esclusivamente impiegate da parte degli utenti e ciascuno ne è responsabile del corretto utilizzo. Non ne è consentito l’uso da parte di persone non autorizzate. Dell’osservanza della presente norma risponde il responsabile di ciascun servizio

3.2 - Le unità di memorizzazione di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Su queste unità, il SII deve svolgere regolari attività di controllo, amministrazione e backup.

3.3 - Le password d'ingresso alla rete ed ai programmi sono segrete e sono comunicate e gestite secondo le procedure impartite all’articolo 4.

3.4 - Il Responsabile del SII 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 (in tal caso è necessario il preavviso da parte del responsabile agli eventuali interessati).

3.5 - Costituisce buona regola di gestione delle unità di memorizzazione di rete da parte degli utenti, la periodica (almeno ogni tre mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione multipla dei dati, al fine di non incrementare inutilmente lo spazio disco ed agevolare le copie di sicurezza.

3.6 - Non è consentito collegare qualsiasi dispositivo alla rete aziendale senza la preventiva autorizzazione scritta del Responsabile del SII previa verifica della conformità agli standard tecnici presenti.

3.7 - Non è consentito all'utente modificare le caratteristiche impostate sui PC forniti, i punti rete di accesso e le configurazioni delle reti LAN/WAN presenti nelle sedi; eventuali modifiche strutturali che si rendessero necessarie dovranno essere concordate con il SII per garantire la compatibilità con la struttura preesistente.

Art. 4 - Gestione delle Password

4.1 – La gestione delle password è regolata dal Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del Dlgs 196/03) e da quanto previsto dal documento programmatico sulla sicurezza adottato dal Comune di Pontedera.

4.2 - La password è strettamente personale e deve essere custodita dall'utente con la massima diligenza e non divulgata.

Le password di ingresso alla rete, di accesso ai programmi e dello screen saver, sono attribuite inizialmente dal Responsabile della gestione e manutenzione degli strumenti elettronici e devono essere immediatamente sostituite dagli utenti.

4.3 - Le password devono essere lunghe almeno 8 caratteri, salvo particolari impedimenti tecnici specifici delle applicazioni, formate da lettere maiuscole e/o minuscole, numeri e caratteri speciali quali & % ^ # $, ricordando che lettere maiuscole e minuscole hanno significati diversi per i sistemi, evitando ovviamente contenuti di senso logico immediato che sono facilmente individuabili (per es. nomi/date di nascita e simili).

4.4 - Le password utilizzate dagli utenti hanno una durata massima di 6 mesi, che è pari altresì a 3 mesi per quegli utenti che trattano dati sensibili e/o giudiziari trascorsi i quali devono essere sostituite.

Ogni nuova password deve essere fornita, in busta chiusa, all’incaricato della custodia delle credenziali.

4.5 - La password deve essere immediatamente sostituita, dandone comunicazione all’incaricato della custodia delle credenziali, nel caso si sospetti che la stessa abbia perso la segretezza.

4.6 - Qualora l'utente venga a conoscenza delle password di altro utente, è tenuto a comunicarglielo immediatamente in modo che possa modificarle ed, in caso di impossibilità, di comunicarlo al suo responsabile che lo comunicherà al responsabile del SII, nelle modalità descritte al punto 2.11, per la disabilitazione temporanea dell’utente.

4.7 - E' dato incarico ai dirigenti di comunicare tempestivamente eventuali cambi di mansione che comportino modifiche o revoche di autorizzazione all'accesso delle risorse informatiche, all'ufficio del personale che lo comunicherà al responsabile del SII nelle modalità descritte al punto 2.11.
4.8 - Il presente articolo costituisce diretta applicazione del punto 5–6 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al D. lgs. 196/03) cui si rinvia per quanto non espressamente previsto.

Art. 5 - Utilizzo dei supporti di memorizzazione removibili

5.1 - I dati sensibili o giudiziari, contenuti in supporti di memorizzazione removibili riutilizzabili (cassette, cartucce, floppy, supporti dati e Usb etc.), se non necessari allo specifico trattamento e non più utilizzati devono essere distrutti o resi inutilizzabili. Detti supporti possono essere riutilizzati da altri incaricati, non autorizzati al trattamento dei dati precedentemente memorizzati, se queste informazioni non sono intelligibili e tecnicamente in alcun modo ricostruibili. Il SII dovrà fornire opportuno supporto per ottenere i risultati attesi.
5.2 - I supporti removibili contenenti dati sensibili e giudiziari sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendano temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettano di identificare gli interessati solo in caso di necessità .
5.3 - Non è consentito leggere 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 da parte del SII.

Art. 6 - Utilizzo Stampanti

6.1 - 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 molto lunghi o di contenuto grafico su stampanti comuni
6.2 – Non è consentito stampare documenti personali su qualsivoglia stampante.

Art. 7 - Utilizzo di PC portatili e/o accessori temporaneamente assegnati

7.1 - L'utente è responsabile del PC portatile e/o accessori (macchina fotografica, videoproiettore) temporaneamente assegnati dal Responsabile del SII e deve custodirli con diligenza sia durante gli spostamenti sia durante l'utilizzo fino alla loro riconsegna
7.2 - 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.
7.3 - I PC portatili utilizzati all'esterno(convegni etc.), contenenti dati dell'ente, devono essere custoditi in un luogo protetto.
7.4 - Eventuali configurazioni di tipo Accesso Remoto sui PC portatili, mediante linea telefonica sono a cura del SII. E' vietato utilizzare le suddette connessioni all'interno delle sedi comunali se contemporaneamente tali PC sono connessi alla rete LAN per la potenziale pericolosità di una doppia apertura verso l'esterno.
7.5 I beni strumentali temporaneamente assegnati devono essere riconsegnati nei tempi stabiliti dall'assegnatario.

Art. 8 - Uso della posta elettronica

8.1 - La casella di posta, assegnata all'utente, è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del loro corretto utilizzo.
8.2 - E' fatto divieto di utilizzare le caselle di posta elettronica …..@comune.pontedera.pi.it per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mailing-lists non attinenti la propria attività o funzione svolta per l'ente, salvo diversa ed esplicita autorizzazione.
8.3 - La posta elettronica deve essere scaricata quotidianamente; in caso di assenza prolungata se ne deve dare comunicazione al responsabile del SII, nelle modalità descritte al punto 2.11, per l'opportuna manutenzione.

8.4 - Per la trasmissione di file all'interno del Comune di Pontedera è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati: se di dimensioni superiori alla capacità della casella di posta, si può utilizzare le directory di scambio (public) presenti sui file server, notificando a mezzo mail al destinatario la disponibilità del file stesso.
8.5 - E' obbligatorio controllare con il software antivirus i file allegati di posta elettronica prima del loro utilizzo.
8.6 - E' vietato inviare catene telematiche (dette anche di Sant'Antonio).
8.7 - Le informazioni riservate o relative a dati sensibili, se devono essere trasmesse, devono essere opportunamente protette con tecniche di cifratura a chiave asimmetrica..
8.8 - La casella di posta elettronica …..@comune.pontedera.pi.it pur essendo talvolta nominativa non è personale, ma funzionale all'attività assegnata; è pertanto suscettibile di accessi da parte del titolare del trattamento che quindi può venire a conoscenza del contenuto della corrispondenza.

Art. 9 - Uso della rete Internet e dei relativi servizi

9.1 - Il PC 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.
9.2 - E' fatto divieto scaricare software di qualunque tipo prelevato da siti Internet, se non espressamente autorizzato dal Responsabile del SII.
9.3 - 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.
9.4 - E' vietata la partecipazione a forum non professionali, l'utilizzo di chat lines (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.
9.5 – Il SII si riserva di applicare per singoli e gruppi di utenti politiche di navigazione personalizzate in base alle mansioni, al fine di ottimizzare l'uso delle risorse, gli investimenti e le prestazioni delle connessioni esistenti.
9.6 - Non è consentito inoltre la ricerca di documenti informatici e la navigazione nei siti con contenuti di natura oltraggiosa e/o discriminatoria per sesso/etnia/religione/opinione e/o appartenenza sindacale e/o politica.
9.7 – L' utilizzo di internet può formare oggetto di controllo, seppur graduale, rispettando i principi di pertinenza e non eccedenza tenendo conto delle linee guida del Garante sia per posta elettronica che la navigazione internet.

Art. 10 - Protezione antivirus

10.1 - Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico mediante virus o mediante qualunque altro software aggressivo.
10.2 – Pur essendo previsto l' aggiornamento automatico, ogni utente è tenuto a controllare il regolare funzionamento del software antivirus installato, secondo le procedure previste.
10.3 - Nel caso che il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente: sospendere ogni elaborazione in corso senza spegnere il computer e segnalare l'accaduto al Responsabile del SII nelle modalità descritte al punto 2.11.
10.4 - Non è consentito l'utilizzo di pc, floppy disk, cd/dvd, dvd riscrivibili, chiavi usb di dubbia provenienza; in caso di necessità chiedere la validazione dal SII nelle modalità descritte al punto 2.11.
10.5 - 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, dovrà essere consegnato al Responsabile del SII.

Art. 11 - Osservanza delle disposizioni in materia di Privacy

11.1 - E' obbligatorio attenersi alle disposizioni in materia di Privacy in osservanza del D. lgs. 196/03 e del disciplinare tecnico in materia di misure minime di sicurezza.

Art. 12 - Sanzioni

12.1 - Il mancato rispetto o la violazione delle regole contenute nel presente Regolamento è perseguibile in base alla gravità delle violazioni con provvedimenti disciplinari previste dal Regolamento del Comune di Pontedera “Sanzioni amministrative per la violazione di regolamenti, ordinanze, determinazioni” nonché con le azioni civili e penali previste dalla normativa vigente in materia.

Art. 13 - Individuazione di ruoli

13.1 - Occorre precisare che all’approvazione del presente regolamento, secondo quanto previsto dal documento programmatico sulla sicurezza adottato dallo stesso Ente, il Responsabile dell' Ufficio Sistema Informativo ed Innovazione è il Dirigente del V° settore “Governance”; il Responsabile della gestione e manutenzione degli strumenti elettronici è il funzionario dell’Ufficio Sistema Informativo ed Innovazione; l’incaricato della custodia delle credenziali è il funzionario dell’Ufficio Sistema Informativo ed Innovazione; altresì l’incaricato delle copie di sicurezza delle banche dati è un dipendente dell’Ufficio Sistema Informativo ed Innovazione salvo che tale attività non sia stata demandata all' Unione dei Comuni della Valdera.

13.2 Qualora vi fossero modifiche nell’individuazione delle persone responsabili, si intende responsabile la persona che pro-tempore riveste il ruolo.