Allegato A) - Regolamento per l'utilizzo degli strumenti informatici.

Introduzione

Le realtà aziendali private e pubbliche si caratterizzano per l'elevato uso della tecnologia informatica che da un lato ha consentito l'introduzione di innovative tecniche di gestione dell'impresa, dall'altro ha dato origine a numerose problematiche relative all'utilizzo degli strumenti informatici forniti al dipendente per lo svolgimento delle proprie mansioni.

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

In questo senso, viene fortemente sentita dalle organizzazioni 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 l'Ente 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 dell'Ente di proteggere la propria organizzazione, essendo i computer aziendali 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. n. 196/03 sulla tutela dei dati personali.

Premesso quindi che l'utilizzo delle risorse informatiche e telematiche del Comune deve sempre ispirarsi al principio della diligenza e correttezza - comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro - il presente regolamento interno è diretto ad evitare che comportamenti talvolta anche inconsapevoli possano innescare problemi con minacce alla sicurezza del trattamento dei dati.

Le prescrizioni qui contenute, non si sostituiscono alle specifiche istruzioni che riguardano l'attuazione del Codice sulla Privacy, ma le integrano.

Il presente regolamento è pertanto diretto a tutelare il Comune di Spinea e ad evitare comportamenti scorretti.

Articolo 1 - Utilizzo del personal computer

Il personal computer affidato al dipendente o al collaboratore del Comune 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 al personal computer è protetto da password, che deve essere custodita dal dipendente con la massima diligenza e non divulgata.

La stessa password deve essere utilizzata ogni qualvolta necessaria per l'accesso alla rete ed alle applicazioni.

Non è consentito l'uso di programmi diversi da quelli caricati ufficialmente dal Comune sui vari elaboratori e ciò in osservanza anche delle norme relative alla tutela giuridica del software e di tutela del diritto d'autore.

Non è consentito installare autonomamente programmi provenienti dall'esterno. Tutte le installazioni devono essere eseguite direttamente dall'amministratore di sistema, ovvero – per gli utenti che siano amministratori del proprio computer - concordate preventivamente con l'amministratore medesimo.

Ciò in quanto sussiste il grave pericolo di introdurre virus informatici e di alterare la stabilità delle applicazioni del proprio personal computer e della rete informatica comunale.
Non è consentito al dipendente od al collaboratore di modificare le caratteristiche impostate sul proprio personal computer, salvo previa autorizzazione esplicita dell'amministratore del sistema.
Il personal computer deve essere spento ogni sera prima di lasciare l'ufficio o in caso di assenza prolungata 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. Pertanto, ciascun computer, se incustodito, deve sempre essere bloccato da password.
Non è consentita l'istallazione sul proprio personal computer di nessun dispositivo di memorizzazione, comunicazione o altro se non con l'autorizzazione espressa dell'amministratore di sistema.
È vietato l'accesso contemporaneo con lo stesso account da più personal computer.
Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente l'amministratore del sistema nel caso in cui siano rivelati virus e seguendo quanto previsto dal presente regolamento relativamente alle procedure di protezione antivirus.
Non è consentita la memorizzazione dei documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.
Non è consentito all'utente di modificare le caratteristiche impostate sui PC assegnati, i punti rete di accesso e le configurazioni delle reti LAN/WAN presenti nelle sedi, salvo autorizzazione esplicita dell'amministratore di sistema.

Articolo 2 - Utilizzo della rete informatica

Le aree comuni disponibili in 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 questa unità vengono 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 PC e sulle cartelle di rete condivise dati aziendali, banche dati e documenti sensibili senza esplicita autorizzazione dell'amministratore di sistema e senza l'adozione di adeguate politiche di sicurezza, quali la criptazione dei dati stessi e l'adozione di politiche di backup comprensive della dotazione di idonei archivi protetti.
I dati estratti ai fini di elaborazioni vanno cancellati entro 30 giorni dalla fine del trattamento degli stessi.
Le password d'ingresso alla rete ed ai programmi sono segrete e vanno gestite secondo le procedure impartite. È assolutamente proibito entrare nella rete e nei programmi con nomi di altri utenti.
L'amministratore del sistema può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza sia dei personal computer dei dipendenti, sia delle unità di rete.
Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con la cancellazione dei file obsoleti od inutili.
Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente da evitare un'archiviazione ridondante, per problemi di occupazione di spazio, ma soprattutto al fine di garantire l'affidabilità degli eventuali dati forniti a terzi.

E’ 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 file di contenuto grafico) su stampanti comuni. In caso di necessità la stampa in corso può essere cancellata dall’amministratore del sistema.
Non è consentito collegare reti di PC od altri dispositivi alla rete aziendale senza la preventiva autorizzazione scritta dell'amministratore di sistema ed una verifica della conformità agli standard tecnici presenti.

Articolo 3 - Gestione delle password
Le password devono essere formate almeno da combinazioni di lettere maiuscole, lettere minuscole e di numeri, ricordando che le lettere maiuscole/minuscole hanno significati diversi per il sistema e che non è possibile inserire il nome, il cognome e l’utente come password o parte di essa. Possono contenere anche caratteri speciali o di punteggiatura.
Le password hanno una durata massima di 90 giorni, trascorsi i quali le password devono essere sostituite e non potranno essere riutilizzate per un anno.
Qualora si sospetti che la password abbia perso la segretezza, essa deve essere immediatamente sostituita.
Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia all’utente stesso ed all’amministratore di sistema.
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 all'amministratore di sistema, per iscritto, al fine di rendere possibili le modifiche dei profili di accesso alle risorse e la sostituzione delle password, ove necessario.

Articolo 4 - Utilizzo dei supporti magnetici
Tutti i supporti magnetici riutilizzabili contenenti dati personali devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato. Una persona esperta potrebbe infatti recuperare dati memorizzati anche dopo la loro cancellazione logica.
I supporti magnetici contenenti dati sensibili devono essere custoditi in archivi chiusi a chiave.
Non è consentito scaricare file contenuti in supporti magnetici/ottici non aventi alcuna attinenza con la propria prestazione lavorativa.
Tutti i file di provenienza incerta od esterna, ancorché 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 Responsabile del Servizio Sistemi Informativi e/o del suo staff tecnico.

Articolo 5 - Utilizzo di PC portatili e di dispositivi telefonici mobili.
L'utente è responsabile del PC portatile assegnatogli dal Comune 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 personal computer connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso, ove ne sussista la necessità, prima del loro collegamento alla rete ovvero della riconsegna.
I PC portatili utilizzati all'esterno, in caso di allontanamento, devono essere custoditi in luogo protetto.

Eventuali configurazioni di tipo Accesso Remoto, dirette verso la rete aziendale o attraverso internet, devono essere autorizzate e predisposte esclusivamente a cura dell'Amministratore di sistema. E' vietato utilizzare le suddette connessioni all'interno delle sedi comunali se contemporaneamente connessi alla rete LAN.

Articolo 6 - Uso della posta elettronica

La casella di posta assegnata dal Comune di Spinea 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 del Comune per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mailing-list.

E' vietato l'utilizzo della casella di posta elettronico per l'invio di messaggi 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 per la Società ovvero contenga documenti da considerarsi riservati in quanto contraddistinti dalla dicitura "strettamente riservato" od analoga dicitura, deve fare riferimento alle procedure in essere per la corrispondenza ordinaria.

Per la trasmissione di file all'interno del Comune è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati; se questi sono di dimensioni consistenti si consiglia di utilizzare lo spazio intranet, secondo le consuete modalità, notificando a mezzo mail al destinatario la disponibilità del file stesso.

È obbligatorio controllare i file allegati di posta elettronica prima del loro utilizzo. Si raccomanda di non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti.

È vietato inviare catene telematiche (c.d. Catene di Sant'Antonio). Se si dovessero ricevere messaggi di tale tipo, si deve comunicarlo immediatamente all'amministratore del sistema. Non si devono in alcun caso attivare gli allegati di tali messaggi.

Ogni utente è responsabile penalmente e civilmente del contenuto della propria casella di posta elettronica.

L'accesso alla posta elettronica a mezzo di dispositivi mobili è consentito purché i dispositivi siano protetti da password. Nel configurare i dispositivi per la posta elettronica il sistema in automatico tenterà di applicare impostazioni di sicurezza e all'utente verrà chiesto di accettare le condizioni di sicurezza; in caso di risposta affermativa potrà utilizzare la posta elettronica da dispositivo mobile.

Articolo 7 – Posta elettronica certificata

Il Comune di Spinea è dotato di caselle di Posta Elettronica Certificata da utilizzare per le comunicazioni ufficiali per le quali sia indispensabile avere un riscontro formale dell'avvenuto invio e della conseguente ricezione.

Le mail ricevute attraverso le caselle di posta elettronica certificata devono essere, di norma, protocollate secondo le procedure all'uopo specificatamente predisposte. Non verranno protocollate quelle comunicazioni che, pur se ricevute a mezzo PEC, non rivestano carattere di ufficialità tale da giustificare la loro acquisizione al protocollo dell'Ente.

Sono attualmente previsti diversi referenti per ciascun indirizzo di posta elettronica certificata, secondo le indicazioni fornite dal Responsabile di Settore competente per materia.

Ogni referente è responsabile penalmente e civilmente del contenuto della propria casella di posta elettronica.

Articolo 8 - Uso della rete Internet e dei relativi servizi

Il personal computer abilitato alla navigazione in Internet costituisce uno strumento 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 vietato al dipendente lo scarico di software gratuiti (freeware) e shareware prelevati da siti Internet, se non espressamente autorizzato dall'amministratore di sistema.

E' 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, di bacheche elettroniche e le registrazioni in guestbooks anche utilizzando pseudonimi (nickname). Inoltre, non è consentita la navigazione in siti ove sia possibile rivelare le opinioni politiche, religiose o sindacali dell'utilizzatore, né visitare siti e memorizzare documenti informatici dai contenuti di natura oltraggiosa e/o discriminatoria

L'accesso ai social network è consentito solo ed esclusivamente per utilizzi che abbiano attinenza diretta con lo svolgimento delle proprie mansioni lavorative.

Articolo 9 - Protezione antivirus

Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico del Comune derivante da virus o da altro software aggressivo.

Ogni utente è tenuto a controllare il regolare funzionamento e l'aggiornamento periodico del software installato, secondo le procedure previste.

Nel caso in cui 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 all'amministratore di sistema.

Non è consentito l'utilizzo di cd rom, cd riscrivibili, nastri magnetici di provenienza ignota.

Ogni dispositivo magnetico di provenienza esterna al Comune dovrà essere verificato mediante programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere consegnato all'amministratore di sistema.

Articolo 10 - Le procedure di back up

L'amministratore di sistema è tenuto ad organizzare le procedure ritenute necessarie e sufficienti per garantire la conservazione ed il ripristino dei dati contenuti nel sistema nel caso si realizzino alcuni dei rischi incombenti sui dati (guasto tecnico, errore umano, dolo).

Sono esclusi i dati contenuti nei singoli elaboratori, per i quali ciascun utente consegnatario dovrà provvedere periodicamente, in accordo con l'amministratore di sistema.

E' compito degli incaricati dei singoli trattamenti di informare l'amministratore del sistema dell'esistenza di nuovi dati da inserire nelle procedure standard di back_up.

E' compito dell'amministratore di sistema di:

- organizzare le aree soggette a back up aziendale
- stimolare gli eventuali investimenti informatici necessari
- organizzare le procedure di copia periodica dei dati su altri computer o altri dischi

- organizzare le procedure di copia periodica dei dati su supporti esterni (CD e simili)
- organizzare le procedure di ripristino dei dati in caso di guasti
- organizzare periodicamente i test di controllo sulla effettiva funzionalità delle procedure adottate
- per quanto riguarda i singoli personal computer in uso agli utenti, fornire loro il necessario supporto per il back up periodico dei dati ivi contenuti.

Articolo 11 – Comunicazioni sindacali

Le OO.SS. possono utilizzare per tutte le comunicazioni di loro competenza lo specifico spazio appositamente istituito all'interno della rete intranet comunale, dove le RSU possono caricare tutti i materiali legati alla loro attività sindacale.

È fatto divieto di utilizzare a scopo sindacale la posta elettronica dell'Ente, se non per le comunicazioni che vengano direttamente inoltrate dalle rappresentanze sindacali (RSU) all'Amministrazione Comunale, nell'ambito dei rapporti contrattuali.

Art. 12 – Utilizzo di strumenti diversi

All'interno degli uffici è vietato l'uso di strumenti informatici che non siano quelli messi a disposizione dall'Ente.

Articolo 13 - Osservanza delle disposizioni in materia di Privacy

E' obbligatorio attenersi alle disposizioni in materia di Privacy e delle misure minime di sicurezza, come indicato nei documenti di individuazione degli incaricati del trattamento dei dati.

I documenti e tutti i materiali presenti sul sistema informatico comunale sono, di norma, liberamente accessibili e non filtrati, ma il loro utilizzo deve avvenire esclusivamente per ragioni d'ufficio, in considerazione del proprio ruolo, nonché dei compiti e delle mansioni affidate.

Non sono ammessi accessi impropri.

In applicazione delle vigenti disposizioni sulla gestione dei flussi documentali, tutti gli accessi e le operazioni compiute sui documenti gestiti sono registrati nei log di processo, con specifica indicazione dell'utente.

Articolo 14 - Inosservanza del regolamento

Il mancato rispetto delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

Art. 15 – Codice disciplinare

Il presente regolamento costituisce integrazione del codice di comportamento dei dipendenti dell'ente e pertanto verrà divulgato e messo a disposizione dei dipendenti secondo le disposizioni vigenti.