COMUNE DI SALA BOLOGNESE
Provincia di Bologna

Regolamento per l'utilizzo degli strumenti e dei servizi informatici e telematici dell'Ente

Approvato con deliberazione della Giunta Comunale n. 124 del 19/11/2010

Pubblicato all'albo pretorio per 15 giorni dal 22/11/2010 al 7/12/2010

Regolamento per l'utilizzo degli strumenti e dei servizi informatici e telematici dell'Ente

INDICE

TITOLO I. PRINCIPI GENERALI

Art. 1. Finalità e ambito di applicazione

1. Il presente Regolamento disciplina le condizioni per il corretto utilizzo degli strumenti informatici forniti dall'Ente al dipendente per lo svolgimento delle proprie mansioni, in conformità alla vigente normativa di settore e alla contrattazione collettiva.

Art. 2. Definizioni

1. Ai fini del presente Regolamento si intende per:
   a) backup: copia di sicurezza dei dati;
   b) chat line: sistema accessibile tramite Internet, che consente di parlare con altre persone via computer;
   c) codice maligno o malware: qualsiasi software creato con il solo scopo di causare danni, più o meno gravi, al computer su cui viene eseguito;
   d) crittazione: metodo di codifica dei dati che impedisce l'accesso ai non autorizzati;
   e) guestbook: libro degli ospiti, utilizzato per lasciare i propri dati su un sito, di solito per esprimere un giudizio;
   f) PDA: sistemi palmari o comunque portabili (es. cellulari di ultima generazione);
   g) programmi di file sharing-p2p: programmi che consentono di condividere/scaricare file dalla rete Internet (es. Emule);
   h) rete LAN/WAN: rete di computer locale (es. il Comune) o geografica (es. Regione, Provincia, sedi distaccate…);
   i) screensaver: salvaschermo, ovvero un'immagine che si attiva automaticamente dopo un certo (e definito) numero di minuti di inattività;
   j) SIAT: Servizio Informatico Associato Terred'acqua;
   k) software freeware e shareware: programmi non soggetti a licenza a pagamento, totalmente gratuiti o gratuiti solo per alcuni giorni;
   l) spamming: sistema che consiste nell'invio di una stessa e-mail, contenente di solito pubblicità, a un numero indefinito di persone;
   m) trojan horses: programmi apparentemente normali e spesso non bloccabili dai sistemi di protezione comuni che, una volta installati sul proprio computer, eludono le difese degli antivirus, consentendo l'ingresso ad altri virus;
   n) worms: sinonimo di virus informatico; un worm è una particolare categoria di programmi in grado di autoreplicarsi, di file in file e di sistema in sistema, usando le risorse di sistema e rallentando il computer.

Art. 3. Obblighi di vigilanza

1. Il Responsabile di Area adotta le misure organizzative opportune per evitare 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. Il Responsabile del Servizio, nei limiti delle sue funzioni di coordinamento e controllo sull'attività degli uffici e del personale, assegnate ai sensi del Regolamento di Organizzazione, vigila sull'utilizzo conforme delle risorse informatiche da parte dei dipendenti.

Art. 4. Divieto di discriminazione

1. Non è consentito visitare siti e/o memorizzare documenti informatici dai contenuti di natura oltraggiosa e discriminatoria per sesso, etnia, religione, opinione, appartenenza sindacale e politica.

Art. 5. Utilizzo degli strumenti e dei servizi informatici e telematici a scopi privati, commerciali o propagandistici

1. E' vietato utilizzare gli strumenti informatici comunali al fine di custodire, far circolare o promuovere materiale pubblicitario personale, codice maligno (virus, trojan horses), programmi pirata o altre porzioni di codice maligno e/o altro materiale non autorizzato.
2. E' vietato copiare o mettere a disposizione di altri, materiale protetto dalla legge sul diritto d'autore (documenti, file musicali, immagini, filmati e simili) di cui l'Ente non abbia acquisito i diritti

TITOLO II. NORME DI COMPORTAMENTO

CAPO I. UTILIZZO DEL PERSONAL COMPUTER

Art. 6. Obblighi di custodia

1. Il personale deve custodire la propria strumentazione in modo appropriato e diligente, segnalando tempestivamente ogni danneggiamento, furto o smarrimento al proprio Responsabile.
2. Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. In caso di assenza temporanea, deve essere attivato lo screen saver con la relativa password.

Art. 7. Gestione delle password

1. Le password di ingresso all'elaboratore, alla rete, di accesso ai programmi e dello screen saver sono assegnate dal SIAT. È prevista l'autonoma sostituzione da parte degli utenti delle password inizialmente assegnate.
2. La password deve essere custodita dall'incaricato con la massima diligenza e non divulgata.
3. Le password utilizzate dagli incaricati al trattamento hanno una durata massima di 6 mesi, trascorsi i quali devono essere sostituite, così come nel caso si sospetti che la stessa abbia perso la segretezza.
4. Qualora un utente venisse a conoscenza delle password di altro utente è tenuto a darne immediata notizia al SIAT o al proprio Responsabile di Area.
5. E' dato incarico ai Responsabili di Area di comunicare tempestivamente al SIAT eventuali cambiamenti organizzativi (dimissioni, pensionamenti, cambio di mansioni e/o ufficio, ecc.) che comportino modifiche o revoche di autorizzazione all'accesso delle risorse informatiche, al fine di rendere possibili le modifiche dei profili di accesso alle risorse e la sostituzione delle password ove necessario.
6. Ogni utente deve indicare all'ufficio competente in base all'organizzazione dell'Ente un collega designato come di propria fiducia che, nel caso di assenza prolungata dal lavoro o

di necessità dell'Ente, può accedere al proprio profilo e alla casella di posta elettronica. Tale accesso verrà consentito dal SIAT dietro richiesta scritta del Responsabile di Area, azzerando la password precedentemente impostata e assegnandone una provvisoria. In assenza della designazione di un fiduciario e a fronte di reali necessità dell'Ente, il SIAT procede ad autorizzare l'accesso alla persona indicata dal Responsabile di Area.

Art. 8. Installazione di software

1. È vietato l'uso di programmi diversi da quelli distribuiti ufficialmente dal SIAT, in conformità a quanto previsto dal D.lgs. 518/92 sulla tutela giuridica del software e dalla L. 248/2000, recante Nuove norme di tutela del diritto d'autore.
2. È vietato installare autonomamente programmi provenienti dall'esterno senza la preventiva autorizzazione del SIAT, su richiesta, anche via mail, del Responsabile dell'unità cui è assegnato il Personal Computer.
3. È richiesta la preventiva autorizzazione del SIAT, su richiesta, anche via mail, dei Responsabili di Area interessati, per l'acquisto o la dotazione di software applicativi e/o procedure pertinenti esclusivamente ad alcune Aree.
4. È vietato all'utente e ai Responsabili di Area modificare le caratteristiche impostate sui Personal Computer assegnati, i punti rete di accesso, le configurazioni delle reti LAN/WAN presenti nelle sedi e la configurazione del Browser per la navigazione, salvo autorizzazione esplicita del SIAT.

Art. 9. Installazione di hardware

1. È vietata l'installazione sul proprio Personal Computer o il collegamento sulla rete LAN di dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, personal computer portatili, telefoni cellulari, PDA ed apparati in genere), salva l'autorizzazione espressa del SIAT, su richiesta, anche via mail, del Responsabile dell'unità cui è assegnato il Personal Computer o il segmento di rete LAN.
2. Ogni utente deve avvertire immediatamente il SIAT nel caso in cui siano rilevati virus sui supporti di origine esterna e attuare quanto previsto dall'articolo 16, relativo alle procedure di protezione antivirus.
3. E' vietato rimuovere, danneggiare deliberatamente o asportare componenti hardware.
4. E' vietato accedere direttamente ad Internet con modem collegato al proprio Personal Computer se non espressamente autorizzati dal SIAT e per particolari motivi tecnici.

Art. 10. Utilizzo dei supporti magnetici

1. I supporti magnetici contenenti dati sensibili devono essere custoditi in archivi chiusi a chiave.
2. Non è consentito scaricare file contenuti in supporti magnetici e ottici non aventi alcuna attinenza con la propria prestazione lavorativa.
3. Tutti i file di provenienza incerta, ancorché potenzialmente attinenti all'attività lavorativa, non devono essere utilizzati o installati o testati. Nel caso di effettiva necessità di impiego devono essere sottoposti a un preventivo controllo e alla relativa autorizzazione all'utilizzo da parte del SIAT.

Art. 11. Utilizzo di Personal Computer portatili

1. L'utente è responsabile del Personal Computer portatile eventualmente assegnatogli dall'Amministratore del Sistema e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
2. Ai Personal Computer 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 prima della riconsegna.
3. I Personal Computer portatili utilizzati all'esterno (ad es. per la partecipazione a convegni), in caso di allontanamento, devono essere custoditi in un luogo protetto.
4. Eventuali configurazioni di tipo Accesso Remoto, dirette verso la rete aziendale o attraverso Internet, devono essere autorizzate esclusivamente dal SIAT.

Art. 12. Procedure di archiviazione e backup

1. Il salvataggio dei dati deve avvenire senza duplicazioni, evitando un'archiviazione ridondante.
2. I dipendenti sono tenuti alla periodica pulizia degli archivi (che deve avvenire almeno ogni sei mesi), con cancellazione dei file obsoleti o inutili.
3. Il personale è tenuto ad osservare le direttive del SIAT volte a garantire il corretto funzionamento delle procedure di backup.
4. I dati, documenti o file creati o modificati attraverso le applicazioni di produttività individuale, ad es. office od open office, devono essere salvati solo sui supporti appositamente destinati sul server (unità di rete con cartelle dedicate agli uffici). Tale disposizione può essere derogata, su richiesta del Responsabile di Area, solo per motivi tecnici.

CAPO II. UTILIZZO DELLE RETI

Art. 13. Utilizzo della rete del Comune

1. Hanno diritto ad accedere alla rete del Comune di Sala Bolognese tutti i dipendenti, gli amministratori, le ditte fornitrici di software e/o servizi per motivi di manutenzione e limitatamente alle applicazioni di loro competenza, collaboratori esterni impegnati nelle attività istituzionali, per il periodo di collaborazione.
2. È vietato dislocare sulle unità di rete dell'Ente qualunque file che non sia legato all'attività lavorativa, nemmeno per brevi periodi.
3. E' proibito entrare nella rete e nei programmi con nomi utente diversi dal proprio.
4. Il SIAT può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza sia sui Personal Computer degli incaricati sia sulle unità di rete.
5. Non è consentito agli utenti collegare reti di Personal Computer o altri dispositivi alla rete dell'Ente senza la preventiva autorizzazione scritta del SIAT.
6. E' vietato agire deliberatamente con attività che influenzino negativamente la regolare operatività della rete e ne restringano l'utilizzabilità e le prestazioni per altri utenti.
7. E' vietato fare, o permettere ad altri di realizzare, trasferimenti non autorizzati di informazioni (software, basi dati, ecc.).

8. E’ vietato installare o eseguire deliberatamente o diffondere su qualunque computer e sulla rete, programmi destinati a danneggiare o sovraccaricare i sistemi o la rete (per esempio virus, cavalli di troia, worms, spamming della posta elettronica, programmi di file sharing - p2p come eMule, e altri).
9. E’ vietato monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività degli utenti, leggere, copiare o cancellare file e software di altri utenti, senza l'autorizzazione del SIAT.
10. E’ vietato usare l'anonimato o servirsi di risorse che consentano di restare anonimi sulla rete.

Art. 14. Uso della posta elettronica

1. I dipendenti assegnatari delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
2. È vietato inoltrare dati ed informazioni classificabili "sensibili" o "riservate" attraverso la posta elettronica, qualora le caratteristiche tecniche della stessa non consentano di garantire la riservatezza delle informazioni trasmesse.
3. E' consentito utilizzare l’indirizzo mail assegnato per invio e ricezione di messaggi anche a carattere personale, purché tale attività avvenga nelle pause o fuori dell’orario di lavoro e sia di modica entità. Anche l’eventuale attività di corrispondenza personale è soggetta all’applicazione del presente Regolamento.
4. Il SIAT ha la facoltà di monitorare lo spazio occupato dalle caselle di posta elettronica sul server e informare gli utilizzatori circa l’opportunità di liberare spazio, invitando alla cancellazione di messaggi, quando lo spazio libero si approssima a zero.
5. Al raggiungimento dell’80% del dimensionamento massimo della casella il SIAT può chiedere al dipendente di cancellare documenti inutili e/o allegati ingombranti. In caso di inerzia del dipendente il SIAT può, previa comunicazione all’interessato, provvedere direttamente alla cancellazione dei file più datati.
6. Non è ammesso l’invio di mail a indirizzi di posta interna al Comune con allegati di peso superiore ai 500 Kb. In questo caso per gli allegati si deve utilizzare la Intranet del Comune oppure un link alle pagine del sito del Comune.
7. E' vietato inviare catene telematiche (o di Sant'Antonio). La ricezione di messaggi di tale tipo deve essere comunicata immediatamente al SIAT o al proprio Responsabile di Area. Non si devono in alcun caso aprire gli allegati di tali messaggi.

Art. 15. Uso della rete Internet e dei relativi servizi

1. E' consentita la navigazione Internet ad uso personale, purché tale attività avvenga nelle pause o fuori dell’orario di lavoro e sia di modica entità. Anche l’eventuale attività di navigazione personale è soggetta all’applicazione del presente Regolamento.
2. E' fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dal SIAT.
3. E' vietata la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guestbooks anche utilizzando pseudonimi (o nicknames), se non attinenti l'attività lavorativa svolta.

Art. 16. Protezione antivirus

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.
2. Ogni utente è tenuto a controllare il regolare funzionamento e l'aggiornamento periodico del software installato, secondo le procedure previste.
3. Nel caso in cui il software antivirus rilevi la presenza di un virus, l'utente deve immediatamente:
a) sospendere ogni elaborazione in corso senza spegnere il computer;
b) segnalare l'accaduto al SIAT.
4. Non è consentito l'utilizzo di floppy disk, cd rom, cd riscrivibili, nastri magnetici di provenienza ignota.
5. Ogni dispositivo magnetico di provenienza esterna all'Ente deve essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, deve essere consegnato al SIAT.

TITOLO III. DISPOSIZIONI FINALI

Art. 17. Controlli

L'utilizzo del Personal Computer, della navigazione Internet e l'uso della posta elettronica saranno memorizzati in appositi spazi sui server comunali in due ambienti separati, protetti da user name e password di amministrazione di sistema; nel primo ambiente saranno memorizzate le informazioni relative a attività svolte dall'utente, navigazioni internet e uso della posta elettronica, il tutto in maniera anonima e non riconducibile alla persona che ha effettuato tali attività; nel secondo ambiente sono invece memorizzati nome utente e computer dal quale sono state svolte le precendenti attività, questo ambiente oltre ad essere protetto da password è anche sottoposto a crittografia, quindi non decifrabile senza apposito codice crittografico.
Tutte le attività del primo ambiente saranno sottoposte al controllo dal personale del SIAT incaricato. Le informazioni del secondo ambiente non saranno lette salvo richiesta specifica dell'Autorità Giudiziaria competente. Nel quale caso sarà fornito tutto il materiale memorizzato compreso l'utente e la postazione attraverso la quale si sono effettuate le attività informatiche.
Le informazioni del primo e del secondo ambiente di monitoraggio sono conservate sui server comunali per un periodo non inferiore ai 6 mesi e non superiore ad 1 anno.

Art. 18. Disposizioni in materia di privacy

1. Agli utenti incaricati del trattamento dei dati sensibili è fatto obbligo di distruggere eventuali copie di sicurezza o supporti di tipo removibile (floppy, CDRom, Nastri) qualora non sia possibile rendere irrecuperabili i dati in essi contenuti.
2. Ai sensi del D.lgs. 196/03 è fatto divieto di divulgazione a qualsiasi titolo delle informazioni presenti nelle banche dati dell'Ente se non disciplinata da appositi protocolli di intesa.
3. Al fine di garantire la corretta gestione delle politiche di sicurezza delle informazioni è fatto divieto di replicare sui dischi locali dei Personal Computer dati aziendali, banche dati e documenti sensibili senza esplicita autorizzazione del SIAT 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.

Art. 19. Sanzioni conseguenti all'inosservanza del Regolamento

1. La violazione da parte dei lavoratori dei principi e delle norme contenute nel presente Regolamento costituisce violazione degli obblighi e dei doveri del dipendente pubblico e, pertanto, in relazione alla gravità dell'infrazione, i Responsabili di Area, previo espletamento di procedimento disciplinare, possono procedere all'applicazione delle sanzioni previste dalle disposizioni contrattuali vigenti in materia.