



COMUNE DI GUSSAGO
Via Peracchia, 3 – 25064 Gussago – BS
Tel 0302522919 – Fax 0302520911 – Email uffurp@gussago.com

Gussago,

Disciplinare tecnico ad uso interno per l'utilizzo degli strumenti informatici e in materia di posta elettronica e internet.

Il presente disciplinare tecnico viene redatto in conformità agli art. 4 e 7 dello Statuto dei lavoratori, all'allegato XXXIV al D.Lgs. 9/4/2008 n. 81 in materia di tutela della salute e sicurezza nei luoghi di lavoro, al Codice in materia di protezione dei dati personali e le norme ivi richiamate, nonché le disposizioni del Garante per la protezione dei dati personali di cui alla deliberazione n. 13 del 1/03/2007 e il provvedimento del Garante del 27/11/2008.

Il Codice in materia di protezione dei dati personali D.Lgs. 196/2003 prescrive ai titolari di trattamento di dati di adottare idonee misure di sicurezza per assicurare la disponibilità e l'integrità di sistemi informativi e di dati, anche per prevenire utilizzi indebiti che possono essere fonte di responsabilità. Inoltre le recenti disposizioni del Garante per la protezione dei dati personali hanno richiamato l'attenzione sulla necessità di verificare le attività dell'Amministratore di sistema attraverso la registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici. D'altro canto la disciplina della protezione dei dati va coordinata con regole di settore riguardanti il rapporto di lavoro e il connesso utilizzo di tecnologie e le norme relative alla sicurezza sul lavoro. Spetta infine al datore di lavoro assicurare la funzionalità e il corretto impiego di strumenti e tecnologia da parte dei lavoratori, definendone le modalità d'uso nell'organizzazione dell'attività lavorativa.

Pertanto

il Comune di Gussago

nel rispetto delle norme sopra riportate e del principio di correttezza del trattamento dei dati personali (art. 11 Codice in materia di protezione dei dati personali),

impartisce istruzioni

circa le modalità d'uso degli strumenti informatici (hardware e software) messi a disposizione dei dipendenti

e

informa i propri dipendenti

sulle funzionalità dei sistemi di sicurezza installati.

1. Utilizzo degli strumenti informatici (hardware)

Il Personal Computer (pc) affidato al dipendente 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, ingenerando, conseguentemente, le responsabilità disciplinari del dipendente.

Il pc deve essere spento ogni giorno al termine dell'orario di lavoro. In caso di assenze prolungate dall'ufficio durante l'orario di lavoro, si devono mettere in atto accorgimenti tali per cui il pc non resti incustodito e accessibile. Al momento dell'intervallo per la pausa meridiana i pc devono essere riavviati e lasciati in blocco, nella fase di attesa di inserimento della password oppure devono essere spenti fisicamente.

In ogni caso lasciare un pc incustodito può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso: la responsabilità ricadrà pertanto direttamente sul dipendente.

E' vietato installare sul proprio pc dispositivi di memorizzazione, comunicazione o altro (masterizzatori, modem, switch, hd esterni, ecc.). Per installare hardware sul proprio pc è necessario richiedere apposita autorizzazione al Dirigente/Responsabile di Area. Tutte le operazioni per l'installazione di hardware devono essere effettuate esclusivamente dal tecnico dei servizi informatici.

Ogni dipendente deve prestare la massima attenzione ai supporti di origine esterna (cd, dvd, chiavi usb, etc.). Prima di utilizzarli è necessario effettuare una verifica con il software antivirus e, nel caso in cui siano rilevati virus, si deve avvertire immediatamente il proprio Dirigente/Responsabile di Area e l'Amministratore di sistema.

Quando vengono utilizzati supporti quali cd, dvd, chiavi usb, etc., si deve prestare la massima attenzione per evitare un utilizzo improprio dei dati personali eventualmente contenuti, custodendoli in armadi chiusi a chiave. Nel caso di trattamento di dati sensibili o giudiziari, i supporti come chiavi usb, cd o dvd già utilizzati, possono essere riutilizzati qualora le informazioni precedentemente contenute non siano tecnicamente in alcun modo recuperabili, altrimenti devono essere distrutti.

I computer portatili devono essere custoditi in un luogo protetto.

La custodia dei supporti fisici delle firme digitali è a totale carico del proprietario: si raccomanda comunque di non lasciarli incustoditi né di comunicare ad alcuno le password di utilizzo.

E' fatto divieto al personale di consentire ad Amministratori, cittadini ed altre persone non autorizzate di utilizzare gli strumenti informatici, pc o videotermini, installati negli uffici.

2. Gestione delle password

L'accesso alla rete e ai software in uso negli uffici è protetto da credenziali di autorizzazione, vale a dire nome utente e password. L'Amministratore di sistema del comune assegna ad ogni dipendente le credenziali di autorizzazione per l'accesso al dominio di rete e per l'accesso a ciascun software in uso negli uffici, credenziali che è vietato diffondere o rendere pubbliche.

Le credenziali sono personali e devono essere custodite con la massima diligenza: i dipendenti dovranno adottare le necessarie cautele per assicurarne la segretezza. Qualora il dipendente sospetti che le credenziali abbiano perso il carattere della segretezza deve darne immediata comunicazione all'Amministratore di sistema che provvederà a sostituirla.

Le password sono composte da almeno otto caratteri e formate da lettere (maiuscole o minuscole) e numeri. Il nome utente deve essere univoco: esso non può essere assegnato ad altri dipendenti, neppure in tempi diversi. Le password di accesso al dominio e ai programmi sono modificate ogni tre mesi, così come disposto dal punto 5 dell'all. B del D.Lgs. 196/2003.

Non appena il sistema richiede il cambio della password, il dipendente è tenuto ad effettuare le operazioni di modifica. Successivamente deve annotare la propria password, inserirla in una busta, sigillarla e scrivere il nome utente sulla busta stessa. La busta va consegnata al Segretario generale. Tutte le buste contrassegnate dai nomi utenti vanno inserite in una busta che viene custodita nella cassaforte posta nell'ufficio segreteria.

Nel caso di prolungata assenza o impedimento del dipendente o qualora l'intervento sia indispensabile e indifferibile in quanto vi sono minacce alla sicurezza del sistema, il Dirigente/Responsabile di Area può autorizzare l'utilizzo delle credenziali del dipendente assente.

Le credenziali di autenticazione e i permessi di accesso devono essere disattivate nel caso in cui il dipendente cessa; nel caso in cui il dipendente venga trasferito ad altro ufficio devono essere modificati i permessi di accesso relativi alle credenziali in possesso del dipendente, in modo da essere conformi agli ambiti di trattamento autorizzati agli incaricati con apposita deliberazione della Giunta comunale.

Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte dell'Amministratore del Sistema.

3. Utilizzo dei programmi informatici (software)

Ogni dipendente ha a disposizione sul proprio pc:

- il sistema operativo Microsoft Windows XX;
- un pacchetto office (software per videoscrittura, fogli di calcolo, etc.);

- browser per la navigazione in internet e per la gestione della posta elettronica;
- software specifico per la gestione della propria attività lavorativa;
- software di visualizzazione di file (pdf, immagini, disegni e video);

E' vietato modificare le impostazioni del sistema operativo e/o dei software.

E' vietato installare autonomamente software. Per installare nuovi software sul proprio pc o per modificare le impostazioni del sistema operativo è necessario richiedere apposita autorizzazione al Dirigente/Responsabile di Area che, se lo riterrà opportuno, farà richiesta all'Amministratore di sistema. Tutte le operazioni per l'installazione di software devono essere effettuate esclusivamente dall'Amministratore di sistema.

Qualora venga rilevato che sui pc dei dipendenti è installato software in violazione delle norme sulla tutela giuridica del software e sul diritto d'autore, tutte le responsabilità connesse ricadranno sul dipendente.

4. Sistema di sicurezza informatico

Il Comune di Gussago ha ottemperato agli obblighi del Codice privacy installando un sistema completo per la gestione della sicurezza della rete e dei dati ivi contenuti con le seguenti funzionalità:

- all'ingresso del collegamento internet, funziona da firewall, filtrando tutti i tipi di attacchi da virus o spyware, i tentativi di intrusione ad opera di hacker o di utenti non autorizzati;
- crea un backup cifrato della configurazione per ripristinare rapidamente la completa operatività del firewall e una copia esatta di tutti i dati su due dischi per garantire una maggiore sicurezza in caso di guasto hardware ai dischi;
- gestisce connessioni multiple a internet, spostando tutto il traffico su una connessione di back up in caso di guasto;
- è dotato di un sistema di aggiornamento automatico di tutti i moduli critici (definizione dei virus, regole antispam, tabella intrusione hacker, etc.);
- esegue automaticamente la scansione delle mail in entrata e in uscita con filtri antispam e antivirus, bloccando immediatamente i pc che inviano messaggi infetti e segnalando il problema all'Amministratore di sistema;
- gestisce filtri sulla navigazione per ottimizzare l'utilizzo della connessione internet e accrescere la sicurezza della rete, dando la possibilità di impostare nel dettaglio l'accesso alla navigazione (scelta delle fasce orarie, scelta degli utenti, filtro sui siti indesiderati, impedire il download di file pericolosi), e controllare l'utilizzo della banda da parte di ogni IP interno;
- riporta per ogni computer (indirizzo IP) l'elenco dei siti visitati, comprensivo del traffico scambiato e degli orari di navigazione, archiviando i dati all'interno del firewall il tempo necessario alla verifica di eventuali problemi connessi alla sicurezza del sistema;
- opera un monitoraggio centralizzato che permette la raccolta di informazioni riguardanti ogni pc collegato alla rete locale e consente di visualizzare tutti gli accessi effettuati nei computer della rete, per il controllo degli accessi al sistema da parte dell'amministratore e al fine di pianificare interventi di backup o aggiornamenti.

A tale sistema di sicurezza e controllo accede l'Amministratore di sistema che può così effettuare un costante e completo monitoraggio, analizzare lo stato dei servizi, la configurazione e l'utilizzo delle risorse hardware del sistema stesso, così da intervenire tempestivamente in caso di necessità. Se durante i controlli per problemi relativi alla sicurezza e all'integrità del sistema, l'Amministratore di sistema dovesse riscontrare violazioni al presente disciplinare, è tenuto a segnalarle al Segretario generale, che valuterà i provvedimenti necessari. Al sistema di controllo può accedere anche il Segretario generale.

Il sistema informatico dell'Ente è interamente protetto da un software antivirus specifico. Qualora detto software segnali l'intrusione di virus il dipendente deve immediatamente segnalarlo al Dirigente/Responsabile di Area e al tecnico dei servizi informatici.

Il sistema informatico dell'Ente è inoltre dotato di un software di back up per salvataggio dei dati da tutti i server che compongono il sistema ad un server dedicato di back up; il salvataggio è quotidiano. Dal server di back up ogni giorno i dati vengono riversati su 6 hd esterni, uno per ogni giorno della settimana, che vengono custoditi nella cassaforte della segreteria.

La struttura organizzativa e i files relativi all'attività lavorativa di ciascun dipendente sono residenti sui server come segue:

1. cartella Utente "*Nome Cognome*", accessibile dal solo utente;
2. cartella Uffici "*Area/Ufficio*", accessibile da tutto l'ufficio;
3. cartella Pubblica "*Nome Cognome*", accessibile da tutti gli utenti.

Non è più attivo il sistema di salvataggio del disco C dei pc in dotazione ai dipendenti. Pertanto, per ovvie ragioni di sicurezza dei dati, tutti ed esclusivamente i files relativi all'attività lavorativa dovranno risiedere nelle cartelle sopra menzionate ai punti 1, 2 e 3.

Al fine di salvaguardare la libertà e la dignità dei lavoratori, si rende noto che non è consentito salvare dati personali o di terzi che non riguardano l'attività lavorativa nelle cartelle sopra menzionate ai punti 1, 2 e 3. in quanto il Comune di Gussago potrebbe aver accesso a tali dati nel caso si rilevino minacce per la sicurezza o problemi sul sistema informatico.

Best practice nell'uso del sistema informatico dell'Ente

Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. E' infatti assolutamente da evitare un'archiviazione ridondante.

Poiché un server del sistema è dedicato alla gestione della posta elettronica, si raccomanda di tenere in ordine la propria casella di posta, cancellando documenti inutili e, soprattutto, allegati ingombranti.

Per quanto riguarda l'uso della stampante, è buona regola effettuare la stampa dei dati solo se strettamente necessaria. Al fine di evitare l'accesso a dati personali da parte di personale non autorizzato, si raccomanda di ritirare prontamente le stampe dai vassoi delle stampanti in uso agli uffici. E' buona regola evitare di stampare documenti o file non adatti (molto lunghi o non supportati, come ad esempio il formato pdf o file di contenuto grafico). In caso di necessità la stampa in corso può essere cancellata.

5. Posta elettronica e Internet

E' consentito l'uso della posta elettronica e di internet a tutti i dipendenti che ne hanno necessità per lo svolgimento delle loro mansioni e il raggiungimento delle finalità istituzionali del Comune di Gussago.

Navigazione in internet

E' consentito accedere a siti internet solo per ragioni strettamente connesse all'attività lavorativa, per aggiornamento professionale o per reperire informazioni necessarie al raggiungimento delle finalità istituzionali del Comune di Gussago.

A titolo meramente esemplificativo e non esaustivo si riporta un elenco dei siti consentiti:

- tutti i siti istituzionali;
- tutti i siti di fornitori;
- tutti i siti che forniscono aggiornamento normativo;
- i siti dei maggiori quotidiani nazionali e locali;
- i siti di società di formazione dalle quali scaricare opuscoli relativi a corsi frequentati;
- motori di ricerca.

Divieti connessi alla navigazione

Al fine di prevenire rallentamenti nella velocità di navigazione e per motivi di sicurezza dei dati e di protezione dall'attacco di virus, è vietato:

- l'uso della linea internet per lo streaming (audio/video);
- l'uso della linea internet per connessioni audio/video;
- il download di file audio/video;
- il download e l'installazione di programmi, anche se freeware o shareware prelevato da siti internet;
- l'accesso a reti di pc peer to peer, con pagamento o fatturazione a carico del dipendente;
- la registrazione a siti i cui contenuti non siano legati all'attività lavorativa;
- la partecipazione a forum non professionali, l'utilizzo di bacheche elettroniche e le registrazioni a guest books anche utilizzando pseudonimi (nicknames);
- accedere a social network (Facebook, Twitter, Messenger, etc.), utilizzare chat lines o altri comportamenti non attinenti all'attività lavorativa

In particolare per quanto riguarda il download e l'installazione di programmi si ricordano le disposizioni riportate al punto 3.

Posta elettronica

Il Comune di Gussago assegna:

- ad ogni dipendente una casella di posta elettronica personale da utilizzare unicamente per ragioni strettamente connesse all'attività lavorativa o per il raggiungimento delle finalità istituzionali del Comune di Gussago;
- ad ogni ufficio una mail condivisa tra tutti i dipendenti appartenenti all'ufficio stesso.

Al fine di prevenire il trattamento di dati in violazione dei principi di pertinenza e non eccedenza o il trattamento di dati personali anche sensibili riguardanti il dipendente o terzi, si suggerisce di non utilizzare la mail assegnata dall'ente per motivi personali.

Al fine di tutelare in tal senso i diritti del lavoratore e i diritti di terzi, il messaggio di posta elettronica dovrà contenere in calce la seguente dicitura:

- *Nome Cognome del dipendente*
- *Ufficio di appartenenza*
- *Indirizzo e-mail dell'ufficio*
- *Comune di Gussago indirizzo e recapiti telefonici e fax*
- *Il presente messaggio non ha natura personale. L'eventuale risposta potrà essere conosciuta da altro personale dipendente del Comune di Gussago.*

Nel caso di assenze programmate, il sistema invierà automaticamente messaggi di risposta contenenti i riferimenti alla mail di settore e altre modalità di contatto dell'Ente.

In previsione della possibilità di assenza improvvisa o prolungata del dipendente oppure nel caso di improrogabili necessità legate all'attività lavorativa si debba conoscere il contenuto dei messaggi di posta elettronica, il dipendente è tenuto a delegare uno o più colleghi che possano verificare il contenuto dei messaggi e inoltrare quelli ritenuti rilevanti per l'attività lavorativa.

E' vietato inviare catene telematiche (o di Sant'Antonio). Se si dovessero ricevere messaggi di tale tipo, è necessario darne immediata comunicazione all'Amministratore di sistema. Non si deve in alcun caso aprire gli allegati di tali messaggi.

6. Controlli e sanzioni

Al fine di verificare la funzionalità e la sicurezza del sistema e prevenire trattamenti di dati non autorizzati o accessi non consentiti (Titolo V Codice in materia di protezione dei dati personali) il Comune di Gussago si riserva la possibilità di effettuare controlli sul sistema ogniqualvolta lo ritenga necessario oppure nel caso il software di gestione della sicurezza lo segnali.

Per controllare l'effettivo adempimento della prestazione lavorativa e il corretto utilizzo degli strumenti di lavoro (artt. 2086, 2087 e 2104 Codice civile) il Comune di Gussago si riserva la possibilità di effettuare controlli sui pc assegnati ai dipendenti su segnalazione anche verbale del Dirigente/Responsabile di area. Nel rispetto dei principi di necessità, di pertinenza e non eccedenza stabiliti dall'art. 3 del Codice in materia di protezione dei dati personali, nel corso dei controlli il Comune di Gussago tratterà i soli dati indispensabili alla verifica sia del corretto utilizzo delle risorse hardware e software assegnate ai dipendenti, sia del rispetto del presente disciplinare da parte del personale dipendente.

In caso vengano rilevati usi impropri degli strumenti informatici o della rete internet, saranno immediatamente inoltrati avvisi preventivi a tutto il personale dell'ufficio interessato affinché i comportamenti non conformi al presente disciplinare cessino.

Il mancato rispetto o la violazione del presente disciplinare è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

7.

In sede di prima applicazione del presente disciplinare verrà effettuata una ricognizione dei software e dell'hardware installato fino ad oggi dal personale per poi provvedere, sentito il parere del Dirigente/Responsabile di Area, ad eliminare software non necessari all'attività lavorativa.