COMUNE DI BITONTO

(Provincia di Bari)

Disciplinare per l'Uso degli Strumenti Informatici

Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196)
Deliberazione n. 13 del 1° marzo 2007 - Garante per la protezione dei dati personali

Approvato con delibera di Giunta Comunale n. 111 del 18-03-2008

SOMMARIO

Art. 1 - Oggetto e ambito di applicazione

Il presente disciplinare regola:

- le modalità di utilizzo degli strumenti informatici nell'ambito dello svolgimento delle proprie mansioni, dei propri compiti di lavoro e delle attività di ufficio da parte dei dipendenti che hanno in dotazione una stazione di lavoro di tipo personal computer, server, notebook;
- l'individuazione delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione per il trattamento dei dati personali al fine di garantire il rispetto delle vigenti normative in materia e gli adeguati livelli di sicurezza ed integrità del patrimonio informativo dell'Amministrazione Comunale.

Il presente disciplinare integra e non sostituisce le regole di comportamento previste dal Documento Programmatico Sulla Sicurezza e da tutte le altre normative in materia.

Art. 2 - Utilizzo delle postazioni di lavoro

Le postazioni di lavoro affidate al personale dipendente sono uno **strumento di lavoro**. Ogni utilizzo non inerente l'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e minacce alla sicurezza.

Ogni postazione di lavoro **deve avere un assegnatario** ed è consegnata e aggiornata con il software necessario, coperto da licenza d'uso concessa dal fornitore, per lo svolgimento delle attività lavorative.

Ogni dipendente assegnatario di postazione di lavoro può inserire una password all'accensione (password del bios); in tal caso questa password, scritta su carta e conservata in busta chiusta, **deve essere consegnata** al proprio Dirigente. La password sarà utilizzata al solo fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività comunale nei casi in cui si renda indispensabile ed indifferibile l'intervento, ad esempio in caso di prolungata assenza od impedimento del dipendente, che verrà tempestivamente informato dell'intervento di accesso realizzato.

E' vietato agli assegnatari delle postazioni di lavoro, senza la preventiva approvazione del Dirigente e/o del Responsabile di Servizio:

- installare e/o far installare altri programmi oltre quelli in dotazione;
- rimuovere i programmi acquistati dall'ente;
- installare, duplicare o utilizzare i vari software al di fuori di quanto consentito dagli accordi di licenza; al fine di evitare rischi di danneggiamenti del sistema per incompatibilità con il software esistente e nel rispetto della normativa a tutela dei diritti d'autore sul software (D.Lgs. 518/92 sulla tutela giuridica del software e L. 248/2000 contenente nuove norme di tutela del diritto d'autore);
- cancellare, copiare o asportare programmi software per scopi personali;
- installare componenti hardware non compatibili con l'attività istituzionale;

- rimuovere, danneggiare o asportare componenti hardware;
- installare e/o utilizzare modem per il collegamento con altre reti, siano esse pubbliche o private;
- far usare la postazione di lavoro a personale esterno a meno di non essere sicuri della loro identità e della autorizzazione del dirigente ad operare sulla postazione;
- **modificare la configurazione hardware e software della postazione di lavoro;**
- attivare programmi eseguibili via internet, che potenzialmente possono alterare le configurazioni predisposte e comunque tendono ad installare software non richiesto;
- utilizzare i server di rete come stazioni di lavoro;
- utilizzare software di proprietà personale, anche se acquistati e registrati, programmi shareware e/o freeware, scaricati da siti internet, o proveniente da dischetti e CD/DVD allegati a riviste e/o giornali o altro software posseduto a qualsiasi titolo;
- inserire password locali alle risorse informatiche assegnate (come ad esempio password che non rendano accessibile il computer agli amministratori di rete), se non espressamente autorizzati e dovutamente comunicate al Dirigente.

Inoltre è importante che tutti gli **utilizzatori di postazioni di lavoro** adottino i seguenti accorgimenti:

- non lasciare, anche momentaneamente, la postazione di lavoro senza protezione da accessi non autorizzati, al fine di evitare che persone non autorizzate possano accedere ai dati e/o alle applicazioni in maniera fraudolenta (si specifica che per persona non autorizzata si intende anche il dipendente comunale dello stesso ufficio e/o di ufficio diverso a cui non è stato assegnato l'uso della postazione);
- in caso di condivisione di cartelle, autorizzare solo gli utenti interessati;
- non mettere in condivisione con altri utenti, cartelle contenenti file di sistema e mai l'intero disco fisso;
- verificare periodicamente gli archivi, cancellando files obsoleti o inutili;
- non utilizzare supporti riscrivibili già utilizzati su computer sul quale è noto che si siano verificati malfunzionamenti;
- non aprire files che abbiano un nome o una estensione sospetta;
- accertarsi che il programma antivirus sia in funzione e che non sia mai disattivato, né tanto meno disinstallato sulla stazione di lavoro;
- riporre, in caso di assenza dal posto di lavoro, in armadietti o cassetti dotati di serratura i supporti magnetici trasportabili (dischetti, cartucce, CD Rom, DVD, pen-drive, ecc.) contenenti dati;
- riutilizzare i supporti già utilizzati solo se le informazioni precedentemente contenute non siano tecnicamente in alcun modo recuperabili, altrimenti devono essere distrutti;
- effettuare copia dei dati memorizzati sulla propria postazione di lavoro,
- spegnere sempre la postazione al termine della giornata di lavoro o in caso di assenze prolungate dall'ufficio.

Al fine di *prevenire malfunzionamenti causati da virus informatici*, perdita di dati o diffusione non autorizzata di informazioni attinenti i dati trattati dall'Ente, **non è consentito,** senza la preventiva approvazione scritta del Dirigente e la configurazione da parte del Servizio Informatico, **collegare** alla rete del Comune **personal computers portatili**.

Il Dirigente, tramite il Servizio Informatico, può controllare la corretta configurazione delle postazioni di lavoro e impedire la modifica della stessa, utilizzando le tecniche e gli strumenti opportuni.

Art. 3 - Utilizzo della rete locale

Nell'uso della rete locale non sono consentite le seguenti attività:

- agire deliberatamente con attività che influenzino negativamente la regolare operatività della Rete e ne restringano l'utilizzabilità e le prestazioni per altri utenti;
- effettuare trasferimenti non autorizzati di informazioni (software, dati, ecc);
- installare, eseguire o diffondere su qualunque computer e sulla rete, programmi destinati a danneggiare o sovraccaricare i sistemi o la rete (ad es. virus, cavalli di troia, worms, spamming della posta elettronica);
- installare o eseguire programmi software non autorizzati o non compatibili con l'attività istituzionale;
- utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività di altri utenti, per leggere, copiare o cancellare files e software di altri utenti;
- utilizzare software visualizzatori di pacchetti TCP/IP, software di intercettazione di tastiera, software di decodifica password e più in generale software rivolti alla violazione della sicurezza del sistema e della privacy;
- usare l'anonimato o servirsi di risorse che consentano di restare anonimi.

Art. 4 - Utilizzo di Internet

L'accesso ad internet è abilitato su tutte le postazioni di lavoro connesse alla rete locale, indicate dai Dirigenti.

La configurazione dei servizi di accesso ad internet deve essere eseguita esclusivamente dal Servizio Informatico.

La connessione ad internet deve avvenire unicamente per il tramite della rete **RUPAR Puglia** (Rete Unitaria della Pubblica Amministrazione Regionale), che consente gli accessi ad una serie di siti internet di tipo istituzionali. Tale connessione è sottoposta ad un sistema automatico di limitazione attiva e controllo (ad esempio limitazione dei siti navigabili) predisposto automaticamente (per sicurezza) sulla rete RUPAR. Nel caso di necessità ad accedere ad altri siti web, il dipendente deve segnalare la richiesta al proprio dirigente che valutata positivamente provvederà a comunicare l'esigenza al Dirigente del Servizio Informatico.

L'utilizzo imprudente di alcuni servizi della rete internet, anche nell'ambito della normale attività professionale, può essere fonte di particolari minacce alla sicurezza dei dati e all'immagine dell'Ente, per cui nell'uso di internet **sono vietate** le seguenti attività:

- navigare in siti non attinenti allo svolgimento delle mansioni assegnate;
- effettuare ogni genere di transazioni finanziarie personali o acquisti on-line personali;
- scaricare (download) software e file, anche se gratuiti, salvo autorizzazione preventiva ed espressa del dirigente ;
- utilizzare programmi per la condivisione e lo scambio di file in modalità "peer to peer" (Napster, e-mule, winmx, e-donkey, ecc.);
- accedere a flussi in streaming audio/video da internet per scopi non istituzionali (ad esempio ascoltare la radio o guardare video o filmati utilizzando le risorse internet);
- registrarsi a siti i cui contenuti non siano collegati all'attività lavorativa;
- partecipare, per motivi non professionali, a forum;
- utilizzare chat line;
- registrarsi in guest book anche utilizzando pseudonimi;
- memorizzare documenti informatici di natura oltraggiosa o discriminatori;
- svolgere qualsiasi attività intesa ad eludere o ingannare i sistemi di controllo di accesso e/o sicurezza di qualsiasi server interno o pubblico, incluso il possesso o l'uso di strumenti o software intesi ad eludere schemi di protezione da copia abusiva del software, rivelare password, identificare eventuali vulnerabilità della sicurezza dei vari sistemi, decrittare file crittografati o compromettere la sicurezza della rete e internet in qualsiasi modo.

Sono espressamente vietate le connessioni ad Internet su linea telefonica, con modem ed abbonamenti anche personali.

Art. 5 - Utilizzo della posta elettronica

Si intende per account di posta elettronica l'abilitazione all'utilizzo di una casella istituzionale personalizzata, nel dominio **comune.bitonto.ba.it** e delle caselle di posta elettronica certificata (PEC) nel dominio **pec.rupar.puglia.it**.

Le caselle di posta elettronica istituzionale personalizzate sono assegnate a:

- Sindaco
- Assessori
- Presidente e Vicepresidente del Consiglio
- Revisori dei conti
- Segretario Generale
- Direttore Generale
- Dirigenti
- Funzionari.

Per gli altri dipendenti sarà formulata apposita richiesta dal proprio Dirigente al Dirigente del Servizio Informatico.

Una casella di posta elettronica (*account*) è caratterizzato da un nome ed una password. Il nome, in mancanza di altra indicazione, è formato dall'iniziale del nome e dal cognome (per esempio m.rossi per Mario Rossi). La password, generata casualmente, viene comunicata in forma riservata dal Servizio Informatico

all'utilizzatore dell'account e deve da questi essere modificata a propria cura almeno ogni sei mesi.

Le caselle di posta elettronica certificata sono assegnate alle unità organizzative ed hanno un unico dipendente/dirigente assegnatario.

L'assegnazione degli account di posta elettronica implica l'obbligo di utilizzo di tale mezzo di comunicazione per lo svolgimento dei propri doveri di ufficio.

Sono vietati:

- l'utilizzo di posta elettronica per motivi privati e/o per contatti interpersonali tra i dipendenti non inerenti l'uso d'ufficio, nonché l'iscrizione a "catene di Sant'Antonio" elettroniche, mailing list pubblicitarie e simili;
- l'accesso al servizio di posta elettronica internet attraverso mezzi (modem o altro) diversi dal collegamento alla rete informatica dell'Ente;
- la trasmissione a mezzo di posta elettronica di dati sensibili, confidenziali e personali di alcun genere, salvo i casi espressamente previsti dalla normativa vigente in materia di protezione dei dati personali;
- l'apertura di allegati ai messaggi di posta elettronica senza il previo accertamento dell'identità del mittente o con oggetto incoerente per contenuto o linguaggio con il mittente (es. mittente: collega di ufficio ed oggetto in inglese, ecc.) o con estensione .exe, .com, .vbs anche se contenuti in file compressi (.zip);
- l'invio, tramite posta elettronica, di user-id, password, configurazioni della rete interna, indirizzi e nomi dei sistemi informatici, documenti di lavoro «strettamente riservati»;
- l'utilizzo di account di altri provider (libero.it, tiscali.it, virgilio.it, ecc.) per motivi attinenti lo svolgimento delle mansioni affidate;
- l'invio e la memorizzazione di messaggi di natura oltraggiosa o discriminatoria.

L'utente si impegna a non rivelare le proprie credenziali per l'accesso ai servizi di posta elettronica e/o di rete e a non utilizzare il nome utente e la password di altri utenti e a non rivelare notizie, dati o informazioni legate al segreto d'ufficio.

Art. 6 - Utilizzo di parole chiavi

Vi sono diverse categorie di password, ognuna con il proprio ruolo preciso:

a) **password di accensione del PC** (password di BIOS): impedisce l'utilizzo improprio della postazione di lavoro, quando per un qualsiasi motivo non si è in ufficio;
b) **password di rete:** impedisce che l'eventuale accesso non autorizzato ad un PC renda disponibili le risorse dell'ufficio (stampanti, cartelle condivise);
c) **password delle applicazioni informatiche centralizzate:** permette di restringere l'accesso alle funzioni e ai dati al solo personale autorizzato;
d) **password di protezione delle risorse (cartelle) condivise:** impedisce l'accesso a tali risorse da parte di utenti non autorizzati i cui PC siano collegati sulla stessa rete locale ed impedisce la propagazione di virus informatici nella rete locale;

e) **password della casella di posta elettronica:** impedisce che i messaggi di posta elettronica indirizzati ad un utente possano essere letti da utenti non autorizzati;
f) **password del salvaschermo:** impedisce che un'assenza momentanea permetta a una persona non autorizzata di visualizzare il lavoro in corso e/o di accedere ai documenti residenti sulla postazione di lavoro.

La password di tipo a) **deve essere obbligatoriamente consegnata** in busta chiusa al proprio dirigente.

Come scegliere una password

Il metodo più semplice per l'accesso illecito a un sistema consiste nell'indovinare la password dell'utente legittimo. In molti casi sono stati procurati seri danni al sistema informativo a causa di un accesso protetto da password "deboli". La scelta di password "forti" è, quindi, parte essenziale della sicurezza informatica.

Le migliori password sono quelle facili da ricordare ma, allo stesso tempo, difficili da indovinare. Questo genere di password può essere ottenuto, ad esempio, comprimendo frasi lunghe in pochi caratteri presenti nella frase, utilizzando anche segni di interpunzione, caratteri maiuscoli e minuscoli, simboli al posto dei caratteri.

La frase "Nel 1969 l'uomo è andato sulla luna" può, ad esempio, fornire tra le tante possibilità la seguente "N69UèAsL".

Accanto a questa tecnica, per ottenere password ancora più "forti", si possono sostituire le lettere risultanti dalla compressione della frase, con cifre o caratteri che assomiglino alle lettere; ad esempio, la frase "Questo può essere un modo per ricordare la password" diventa "Qp&1mpRP".

Un altro modo per ottenere password "forti" consiste nel combinare date o numeri che si ricordano facilmente con pezzi di parole che sono in qualche modo abituali e quindi semplici da ricordare; ad esempio, la combinazione "felice1983", che utilizzata direttamente potrebbe essere una password "debole" (combinazione del nome del figlio e della data di nascita), può diventare una password migliore in questo modo "FeLi83ce", o una password "forte" così "F&Li83cE".

Art. 7 - Competenze e Responsabilità

I Dirigenti sono tenuti a:

- informare il personale sulle disposizioni in merito all'uso consentito delle risorse del sistema informativo del Comune,
- assicurare che il personale assegnato si uniformi alle regole e alle procedure descritte nel presente disciplinare.

Il Servizio Informatico è incaricato di:

- configurare le postazioni di lavoro per l'accesso alla rete locale e ad internet;
- monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare il corretto utilizzo delle risorse di rete, dei computer e dei programmi

applicativi, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto dei diritti degli utenti;

- rimuovere programmi software e componenti hardware dalle risorse informatiche assegnate agli utenti, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto dei diritti degli utenti;
- utilizzare le credenziali di accesso di amministrazione del sistema o l'account di un utente tramite reinizializzazione della relativa password, per accedere ai dati o alle applicazioni presenti su una risorsa informatica assegnata ad un dipendente in caso di prolungata assenza, irrintracciabilità o impedimento dello stesso. Tale utilizzo deve essere esplicitamente richiesto dal Dirigente del dipendente assente o impedito e deve essere limitato al tempo strettamente necessario al compimento delle attività indifferibili per cui è stato richiesto;
- elaborare le regole per un utilizzo ragionevolmente sicuro del sistema informatico;
- gestire i filtri per la navigazione internet secondo le regole specifiche dettate dal presente disciplinare e secondo le istruzioni fornite dal Segretario Generale al fine di evitare la navigazione su siti non attinenti l'ambito istituzionale e, soprattutto, potenzialmente lesivi per il sistema informatico comunale;
- segnalare al Segretario Generale/Direttore Generale ogni eventuale attività non autorizzata sui sistemi.

Il personale del Comune è tenuto al rispetto delle regole stabilite dall'Amministrazione nel presente disciplinare per l'uso delle risorse informatiche e telematiche ed è responsabile:

- della postazione di lavoro assegnata, del mantenimento della configurazione impostata, delle installazioni hardware e software sulla postazione, dei dati memorizzati,
- dell'uso della navigazione in internet effettuata dalla postazione assegnata, dei contenuti che cerca, dei siti che contatta, delle informazioni che immette e delle modalità con cui opera;
- di qualsiasi azione svolta utilizzando codici identificativi e/o password assegnate.

Art. 8 - Violazioni

Il Comune di Bitonto si riserva il diritto di monitorare e verificare, nel pieno rispetto della normativa vigente, anche saltuariamente o occasionalmente, l'attuazione delle disposizioni del presente disciplinare al fine di salvaguardare l'integrità del proprio sistema informatico.

In caso di comprovata necessità, per esigenze statistiche, per necessità tecniche (ad es. monitoraggio della velocità di trasmissione della rete, controllo occupazione della banda) o per esigenze di sicurezza (ad es. postazioni colpite da virus provenienti da siti non istituzionali) può attivare sistemi che consentono il monitoraggio dei siti visitati dal personale nelle modalità previste dalla normativa vigente. Nell'effettuazione di questi

controlli saranno comunque essere rispettati i diritti alla privacy dei dipendenti sanciti dal D.Lgs. 196/2003 e dalla L. 300/70.

I controlli sono effettuati esclusivamente tramite il Servizio Informatico.

L'Amministrazione si riserva il diritto di addebitare al dipendente le spese derivanti da guasti o malfunzionamenti derivanti dal mancato rispetto delle regole stabilite dal presente disciplinare.

Ogni utente è responsabile civilmente e penalmente del corretto uso delle risorse informatiche, dei servizi/programmi e dei dati ai quali ha accesso.

Nei casi di accertata violazione delle norme, saranno applicati i necessari provvedimenti disciplinari, fermo restando l'obbligo di segnalare alla competente Autorità Giudiziaria eventuali violazioni costituenti reato.

Art. 9 - Aggiornamento e revisione

Tutti gli utenti possono proporre integrazioni al presente disciplinare. Le proposte verranno esaminate dal Segretario Generale congiuntamente al Servizio Informatico.

Il presente disciplinare è soggetto a revisione con frequenza annuale.

Art. 10 - Diffusione

Il presente documento verrà trasmesso al Segretario Generale e a tutti i Dirigenti, che avranno l'obbligo di notificarlo a tutti i dipendenti che utilizzano strumenti informatici per il lavoro d'ufficio a cui sono preposti e verrà affisso all'albo pretorio.