COMUNE DI BITETTO

Medaglia d'oro al Merito Civile

SERVIZIO INFORMATICO COMUNALE

REGOLAMENTO COMUNALE

PER L'UTILIZZO DELLE RISORSE DI RETE INFORMATICA NON DISPONIBILE AL PUBBLICO E SICUREZZA DEI DATI

INDICE

PREMESSA 3
Art. 1 - DEFINIZIONI 3
Art. 2 - UTILIZZO DELLA RETE 4
Art. 3 - IMPOSTAZIONI DELLA RETE 5
Art. 4 - PASSWORD 5
Art. 5 - ABILITAZIONE CODICI IDENTIFICATIVI 7
Art. 6 - PROGRAMMI ANTI-INTRUSIONE 7
Art. 7 INTERNET 8
Art. 8 - DOTAZIONE SOFTWARE 9
Art 9 - ACQUISTI 10
Art. 10 - SICUREZZA LOGICA 10
Art. 11 - REINTEGRO DEI SUPPORTI DI MEMORIZZAZIONE 11
Art. 12 -SICUREZZA FISICA 11

PREMESSA

La presenza sempre più rilevante dell'informatica a vari livelli all'interno della struttura comunale e l'introduzione di una rete di personal computer, tutti dotati di una propria unità elaborativa, introduce l'obbligo di stabilire alcune regole fondamentali di approccio alla nuova filosofia client /server, e di utilizzo del nuovo sistema.

Al fine di limitare i danni e gli inconvenienti che una gestione non corretta del sistema può causare, vengono elencate nel seguito le principali e minime attività e regole da seguire.

Attualmente la rete comunale non è direttamente accessibile dall'esterno, fatti salvi gli occasionali collegamenti alla rete Internet od ai servizi di teleassistenza delle procedure installate e di alcuni settori con Enti istituzionali (Ministeri, Anagrafe tributaria, INPS, MTCC, INA (Indice Nazionale delle Anagrafi), ecc.)

Tutte le postazioni di lavoro trattano, in maniere più o meno preponderante, dati personali e sensibili.

Sulla base di tali presupposti ogni settore, di concerto con il SIC definirà le misure minime di sicurezza per il loro trattamento , secondo le disposizioni dettate dalla normativa vigente sulla tutela dei dati personali (l. 31 dicembre 1996, n. 675, d. lgs. 11 maggio 1999, n. 135; D.P.R. 28 luglio 1999, n. 318).

Il presente regolamento ha, pertanto, come finalità quello di garantire un corretto utilizzo del sistema informativo per gli scopi istituzionali del Comune assicurando, nel contempo, il rispetto delle norme sul trattamento dei dati e la sicurezza degli stessi.

Art. 1 - DEFINIZIONI

Ai fini del presente regolamento s’intende per:

Servizio Informativo Comunale (SIC): il Servizio che sovrintende all'architettura informatica, ne cura lo sviluppo e la gestione.

Amministratore di Sistema: il soggetto al quale è conferito il compito di sovrintendere alle risorse del sistema operativo e di consentirne l'utilizzazione. Tale soggetto utilizza un codice identificativo personale di accesso al sistema gestito secondo le specifiche standard di advanced security, ed è inoltre abilitato ai comandi low-level di sistema operativo.

Assistenti di supporto: sono operatori specializzati in procedure informatiche e, quei dipendenti individuati per iscritto dai Funzionari, che svolgono funzioni elementari di supporto informatico all'interno dei servizi del Settore di appartenenza con compiti di ordinaria manutenzione. Essi, provvedono alle segnalazioni al SIC di problemi hardware e software dei personal computer assegnati, e si rapportano con il SIC per periodici aggiornamenti organizzativo-tecnici del lavoro su reti.

Art. 2 - UTILIZZO DELLA RETE

Le risorse hardware (personal computer, stampanti , server di rete) sono collegate fra di loro secondo un'architettura che consente di coniugare flessibilità e razionalità di utilizzo.
La condivisione di risorse permette, a chiunque ne abbia titolo e secondo specifiche autorizzazioni, l'utilizzo delle risorse disponibili.
Nell’ambito dei supporti di memorizzazione di massa del server il SIC mette a disposizione per ogni Settore delle cartelle condivise, che sono poi rese disponibili sotto forma di unità logiche (tipicamente disco F:) per tutte le postazioni del Settore stesso. Il Funzionario responsabile provvede a comunicare al SIC i livelli di accesso e relative possibilità di utilizzo per ogni singolo utente, nonché eventuali necessità che dovessero presentarsi.
In considerazione del fatto che tali particolari risorse, pur essendo disponibili sulle singole postazioni, di fatto si trovano sul server e, pertanto, permettono di essere copiate sui supporti preposti al backup, nonché eventualmente di essere accessibili anche da altre postazioni gli utenti quindi dovranno riversare (salvare) sulle stesse:

- i propri dati (documenti "finiti") aventi caratteristiche di rilevanza tali da renderne consigliabile il salvataggio su supporti specifici, al fine di garantire la possibilità di un loro recupero in caso di crash della postazione remota
- quei dati per cui si rende auspicabile la possibilità di un accesso condiviso da parte di soggetti e/o postazioni diverse, eliminando la necessità di spostamento fisico di supporti informatici (tipicamente floppy disk)
- quei dati personali e sensibili trattati dai vari Uffici che, per motivi particolari di riservatezza, devono essere ulteriormente tutelati contro l'eventuale furto o tentativo di

manomissione della singola postazione. In questo caso l'utente dovrà altresì provvedere ad eliminare dalla stessa la copia dei dati riversati sul server.

Viceversa, al fine di evitare un inutile spreco di risorse sul server, gli utenti dovranno mantenere sui dispositivi di memorizzazione delle singole postazioni tutti i dati che non hanno le caratteristiche sopra citate.

Art. 3 - IMPOSTAZIONI DELLA RETE

Ogni singolo Personal Computer accede alla rete tramite apposito identificativo fornito dal SIC, ed è univocamente definito da un indirizzo IP. Il SIC conserva apposita tabella contente la relazione fra ogni singola postazione, il suo ID di rete ed il relativo indirizzo IP.
Proprio per consentire le funzionalità dell'architettura (condivisioni, utilizzo di diverse risorse da ogni singola postazione, ecc.) è vietata qualsiasi modifica alle impostazioni, connessioni o condivisioni create dal SIC.

Art. 4 - PASSWORD

Il SIC provvederà ad attribuire, per ogni personal computer, in conformità al D.P.R. n. 318 del 23.07.99, ed ai sensi dell'art.15 della L. 31.12.96 n.675, tre password:

1. password di accesso alla risorsa (tramite controllo del bios di sistema),
2. login e password di accesso alla rete (tramite verifica del dominio NT),
3. login e password di accesso al software applicativo di pertinenza.

Per consentire la funzionalità delle risorse condivise all'interno delle stesso ufficio (stampanti) la password di accesso alla singola risorsa sarà attribuita per ufficio, e diversificata tramite l'aggiunta di un ordinale.
Tutte le password ed i login saranno inseriti ed aggiornati dal SIC di concerto con ogni Responsabile di settore, che provvederà a conservarne l'elenco secondo le modalità previste dalla normativa vigente.

Il Responsabile del Servizio Informatico provvederà ad incaricare per iscritto i dipendenti addetti alla gestione e conservazione delle password.

Tali password non dovranno essere modificate per alcun motivo dall'utente assegnatario, in quanto tale possibilità è consentita esclusivamente al SIC.

Al più tardi ogni sei mesi il SIC provvederà a sostituire le password di rete e di applicazione di ogni singolo utente, disattivando definitivamente e senza possibilità di riutilizzo quelle fino a quel momento in uso. A tal fine il SIC potrà avvalersi anche dei servizi di password expiring forniti dal sistema operativo.

I codici identificativi personali dovranno essere gestiti in modo che ne sia prevista la disattivazione in caso di perdita della qualità che consentiva l'accesso all'elaboratore. Se verrà meno la qualità che aveva consentito l'attribuzione del codice identificativo personale (per esempio risoluzione del rapporto di lavoro) lo stesso codice non potrà essere attribuito a un nuovo dipendente.

I codici identificativi individuali sono strettamente personali e non devono essere comunicati ad alcuno. Sono consegnati individualmente ad ogni dipendente che ne è, pertanto, pienamente responsabile. Qualora il SIC, tramite il normale monitoraggio delle connessioni verificasse che le stesse sono state utilizzate da dipendente diverso rispetto a quello assegnatario, provvederà immediatamente e per iscritto a darne comunicazione al Funzionario responsabile ed al Segretario Generale.

Tale riservatezza è necessaria in quanto il personal computer collegato in rete costituisce un possibile punto di accesso anche per gli altri personal e quindi potrebbe permettere ad altri dipendenti non autorizzati (o a terzi esterni all'Ente) di accedere anche a dati sensibili in evidente violazione delle norme sulla sicurezza dei dati stessi.

E’ fatto assoluto divieto ai dipendenti addetti alla gestione di ogni personal computer dell’utilizzo dello stesso ad altro personale od estranei all’ufficio che non sia dipendente di ditte che abbiano la manutenzione del software o dell’Hardware, dell’apparecchiatura informatica ad essi assegnata.

Al termine dell'orario di lavoro, intendendo per termine anche la sospensione per la pausa del pranzo, o in caso di assenza di durata tale da non consentire la sicurezza dei dati della singola postazione, il personal computer deve essere lasciato in modalità non accessibile da terzi (Lock su sistemi NT, con software apposito o quantomeno con screen sever protetto da password su sistemi Windows 98).

Il SIC è tenuto a segnalare, in forma scritta, ogni mancata osservanza delle direttive al Responsabile del Servizio Informatico.

Art. 5 - ABILITAZIONE CODICI IDENTIFICATIVI

Per l'attribuzione dei privilegi di accesso connessi al codice individuale identificativo che consente l'utilizzo di software applicativo specifico, i Funzionari responsabili di Settore faranno richiesta di accesso e utilizzo, in forma scritta, al SIC, indicando esplicitamente i diversi gradi di capacità (gestione, interrogazione, ecc.) per il Personale incaricato dei vari servizi, elencando inoltre i "menù" (se presenti) del programma ritenuti strettamente necessari alla funzionalità dell'operatore, in relazione alle funzioni a ciascuno assegnate, in adempimento a quanto previsto dalla Legge 675/96 e successivo D.P.R. 318/99 citati.

Nel caso fosse evidenziata dal Funzionario la necessità di accedere, in sola consultazione, ai dati di competenza di altro Settore, la richiesta di abilitazione a tali "menù" dovrà essere approvata e sottoscritta anche del Funzionario responsabile del Settore cui i dati fanno capo.

Il SIC non è tenuto ad abilitare accessi, anche in sola consultazione, in mancanza della richiesta scritta nelle forme di cui sopra.

Art. 6 - PROGRAMMI ANTI-INTRUSIONE

La presenza dei cosiddetti virus è un problema da affrontare con le dovute serietà e cautele e soprattutto con la consapevolezza che il mancato rispetto delle regole può essere dannoso sia al proprio personal, e quindi al proprio lavoro, che a quello degli altri, se non addirittura a quello dell'intero Ente nel caso si " infetti" il server centrale.

Per questo motivo nel presente articolo si descrivono le precauzioni che ciascun utente è tenuto ad osservare.

Su ogni postazione di lavoro viene installato un programma antivirus, che opererà normalmente anche in background per uno scanning continuo dei dati utilizzati. In caso di mancanza o malfunzionamento di questo software (per reinstallazione del sistema operativo o altre cause), l’operatore è tenuto a segnalare la cosa al SIC con la massima urgenza.

Dei programmi "antivirus" già installati vengono fornite, regolarmente e con cadenza quanto meno settimanale, versioni aggiornate, per consentire la massima sicurezza possibile rispetto ai "virus" fino a quel momento noti.

Il SIC è tenuto ad effettuare direttamente , o a comunicare la disponibilità dello stesso. In quest’ultimo caso gli assistenti di supporto sono tenuti ad effettuare tempestivamente le procedure, secondo le

modalità indicate dal SIC, dando conferma scritta allo stesso della regolare esecuzione, segnalando nel dettaglio i virus eventualmente riscontrati.
Nel caso di presenza di virus, anche se rimosso automaticamente, dovrà essere contattato immediatamente il SIC ed il personal computer "infetto" non dovrà essere usato per alcun motivo fino alla bonifica.
Al fine di monitorare il fenomeno, il SIC manterrà un elenco dei virus riscontrati e/o segnalati.
Il software antivirus:

1. non deve essere mai disabilitato;
2. deve risultare attivo per ogni "file";
3. deve essere eseguito su tutto l'Hard Disk,
4. deve essere eseguito ogni volta che viene utilizzato un floppy disk o un CD Rom.

Per agevolare il lavoro degli utenti il SIC potrà predisporre delle procedure automatizzate di scansione da effettuarsi in momenti di inattività degli uffici (tipicamente di notte). In questo caso gli utenti sono comunque tenuti al rispetto assoluto delle disposizioni del penultimo comma dell'art. 4.
Il SIC dovrà segnalare, in forma scritta, al Funzionario responsabile, ogni eventuale anomalia e difformità riscontrata, rispetto a quanto indicato, al fine di adottare i necessari provvedimenti per il mantenimento della sicurezza del Sistema.

Art. 7 INTERNET

Allo stato attuale, su reti LAN chiuse, i rischi maggiori per la sicurezza derivano dall'utilizzo di collegamenti ad Internet operati da postazioni connesse alla rete locale. Per questo motivo queste postazioni devono rispettare protocolli di sicurezza più elevati rispetto a quelli degli altri Personal Computer.
Tutti i PC dotati di modem, e quindi in grado di comunicare con l'esterno, devono essere strettamente monitorati dal SIC, che potrà verificare, tramite l'uso di appositi strumenti software, il tipo e la durata delle connessioni effettuate.
E' fatto assoluto divieto di effettuare connessioni diverse da quelle impostate dal SIC in "Accesso Remoto", anche per motivi di teleassistenza, senza la previa verifica del SIC stesso.

Il SIC predispone le necessarie impostazioni di sistema per l'accesso alla rete Internet e relativi servizi di E-mail. Per i motivi di sicurezza sopra citati, e per impedire l'accesso a persone non autorizzate, gli utenti non dovranno nel modo più assoluto avvalersi delle funzioni di memorizzazione delle password contenute nei programmi di navigazione e client di E-mail.

Durante la navigazione l'addetto dovrà limitarsi ad accedere ai siti connessi con le attività dell'Ente, evitando con particolare cura tutti quelli che non presentino le massime garanzie in termini di sicurezza.

Per ulteriore precauzione le funzioni di verifica dei "cookies", delle applet Java e degli script ActiveX dovranno essere comunque attivate, e l'operatività degli stessi consentita solo se sussistono le condizioni minime di sicurezza previste dal SIC.

Tutto il materiale proveniente da Internet, nonché gli attachment di E-mail, dovranno essere sottoposti a verifica con software antivirus avente le firme aggiornate, essendo estremamente elevato il rischio di contrarre virus anche di recente produzione.

Tutti i Responsabili di Settore, attraverso i propri collaboratori designati a far parte del SIC, dovranno inviare al Responsabile del Sistema Informatico Comunale tutti gli atti prodotti (delibere, determine, regolamenti, comunicati stampa, ecc.) al fine dell'aggiornamento costante del sito del comune. Detti atti devono essere trasmessi con cadenza settimanale da concordare con il SIC.

Art. 8 - DOTAZIONE SOFTWARE

Ogni personal computer e, più in generale, ogni attrezzatura informatica, ha in dotazione software di utilità forniti su rilascio di regolare licenza.

La legge che disciplina i diritti d'autore (L. 22 aprile 1941 n. 633), aggiornata dal Dl. 29.12.1992, n.518, che ha recepito la direttiva CEE n. 250 del 14.05.1991 relativa alla tutela giuridica del software, prevede che la sua duplicazione, salvo apposito contratto, oltre al numero di licenze regolarmente acquistate, sia reato perseguibile anche penalmente. Pertanto ogni software installato sulle attrezzature in dotazione agli Uffici dovrà essere corredato da regolare licenza.

Tutte le licenze, anche quelle che verranno nel tempo acquisite, devono essere consegnate al SIC che ne curerà la registrazione e le conservazioni.

Al fine di tenere aggiornato il patrimonio informatico in dotazione, nonché per rendere più snella l'attività di manutenzione, il SIC predisporrà una scheda, sottoscritta anche dall'utente assegnatario, per ogni singola attrezzatura, indicante le caratteristiche della stessa (marca, modello, numero di matricola, numero di inventario, ecc.) e il software installato.

Ogni software non indicato nella suddetta scheda è da considerarsi privo di regolare licenza e pertanto di ritenere non autorizzato e assimilabile a "software pirata".
E’ fatto assoluto divieto ad ogni addetto di effettuare l’installazione di qualunque tipo di software, anche se dotato di regolare licenza, senza previo assenso del SIC, che verificherà preventivamente le caratteristiche del prodotto e le eventuali ripercussioni che una sua installazione potrebbe avere sul buon funzionamento della singola postazione o dell’intera LAN.
I singoli assegnatari dovranno rispondere di ogni eventuale difformità riscontrata. Il SIC è tenuto a segnalate, in forma scritta per i provvedimenti anche disciplinari dei caso ogni eventuale installazione non registrata.
I supporti informatici di vario genere, spesso allegati gratuitamente a riviste e periodici, non sempre sono di buona qualità. Inoltre alcuni prodotti di tipo "shareware" (cioè privi di licenza) in genere risultano non soggetti a copyright solo per soggetti privati. Perciò, se ne vieta categoricamente l'impiego.
E' vietata l'installazione di programmi di intrattenimento, giochi e quant'altro non attinente all'attività lavorativa.
L'attivazione di screen-saver, in quanto in grado di determinare un notevole degrado di prestazioni in sistemi operativi di tipo "Windows", dovrà essere effettuata con la supervisione del SIC, che curerà altresì che, in mancanza di altro software all’uopo dedicato, siano attivate le funzioni di protezione dello screen-saver medesimo.
Per quanto sopra esposto, il SIC è tenuto ad effettuare periodici controlli su ogni postazione di lavoro e a segnalare in forma scritta eventuali inadempienze.

Art 9 - ACQUISTI

Al fine di garantire la compatibilità delle singole componenti con l'intero sistema informatico e di mantenere una standardizzazione dei prodotti, anche per un miglior utilizzo delle risorse disponibili, per ogni acquisto di materiale informatico, sia hardware che software, dovrà essere acquisito preventivamente il parere di conformità del responsabile dei SIC.

Art. 10 - SICUREZZA LOGICA

Oltre che con le modalità precisate negli articoli precedenti (codici identificativi individuali, autorizzazioni specifiche per l'accesso selezionato ai dati, programmi antivirus, periodici controlli, ecc.)

l'integrità e la sicurezza dei dati devono essere garantite da rischi di distruzione e perdite accidentali (comandi applicativi c/o operativi errati, presenza nonostante tutto, di virus, malfunzionamenti dell'hardware, ecc.).

E' pertanto obbligatorio procedere giornalmente, a cura del SIC, ad effettuare le procedure di salvataggio, adottando un sistema di rotazione dei supporti e garantendone la conservazione periodica in luoghi ignifughi e blindati (armadio blindato o cassaforte).

Art. 11 - REINTEGRO DEI SUPPORTI DI MEMORIZZAZIONE

Considerata la difficoltà di mantenere una netta separazione fra i dati trattati dagli Uffici, e considerata comunque la non opportunità, anche fortuita, che anche dati non rilevanti per la Legge 675/96 vengano accidentalmente diffusi, i supporti magnetici già utilizzati per il trattamento possono essere riutilizzati qualora le informazioni precedentemente contenute non siano tecnicamente in alcun modo recuperabili, altrimenti devono essere distrutti.

Per la stessa ragione lo smaltimento o la cessione del materiale ormai obsoleto (Hard-Disk, PC, cartucce DAT o MO etc.), potrà essere effettuato solo previa autorizzazione del SIC, che avrà verificato l’impossibilità assoluta di procedere, per eventuali Terzi, al recupero dei dati precedentemente in uso.

Art. 12 -SICUREZZA FISICA

E' preciso dovere di ciascuno, secondo le funzioni e le relative responsabilità, di fare in modo che vengano utilizzati scrupolosamente tutti gli accorgimenti atti ad evitare indebite intrusioni negli edifici comunali (manutenzione e controllo dell'impianto di allarme, chiusura a chiave dei contenitori e dei luoghi ove vengono conservati dati e attrezzature, utilizzo del badge magnetico per l'accesso ai locali dove risulti installato l'apposito lettore, verifica periodica della corretta tenuta di infissi, serramenti e porte d'accesso dall'esterno, posizionamento di estintori in quantità sufficiente e, particolarmente, in prossimità del locale CED e dove sono conservati i supporti per il backup).

E' considerata negligenza , e trattata nei modi previsti dalla normativa vigente, anche la mancata segnalazione di eventuali anomalie casualmente riscontrate da parte di chiunque ne venga a conoscenza.