COMUNE DI FLORIDIA

(Provincia di Siracusa)

SERVIZIO INFORMATICO COMUNALE

REGOLAMENTO COMUNALE PER L'UTILIZZO DELLE RISORSE DI RETE INFORMATICA

INDICE

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 o ai servizi di tele-assistenza delle procedure installate.

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

Sulla base di tali presupposti ogni settore, di concerto con il Sistema Informatico Comunale è chiamato a definire le misure minime di sicurezza per il loro trattamento , secondo le disposizioni dettate dalla normativa vigente sulla tutela dei dati personali.

Il presente regolamento ha, pertanto, lo scopo 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.

È quindi necessario attivare una serie di norme, restrizioni e controlli.

Art. 1 – DEFINIZIONI

Ai fini del presente regolamento s'intende per:

- **Servizio Informatico Comunale (SIC)**: il servizio che gestisce l'architettura informatica all'interno di ogni singola area.
- **Responsabile del SIC:** è colui al quale è conferito il compito di gestire il SIC monitorando e controllando il corretto utilizzo delle risorse di rete, proponendo ai responsabili di settore soluzioni per migliorare la gestione e lo sviluppo del SIC stesso.

Art. 2 – FUNZIONI DEL SISTEMA INFORMATICO COMUNALE

E' fatto obbligo al SIC di svolgere le seguenti funzioni:

a) Gestione software e hardware dei server;
b) Gestione della rete locale;
c) Cura dei seguenti servizi di rete: posta elettronica, web server internet e intranet, IP e DNS, server ftp, server firewall, stampa in rete e connettività locale col protocollo TCP/IP;
d) Monitoraggio attività dei server, del traffico di rete e archiviazione di questi dati;
e) Gestione di periferiche: P.C., Stampanti, Scanner e Plotter;
f) Gestione delle memorie di massa e dei backup dati sui server ;
g) Gestione delle chiamate di assistenza per interventi su hardware e software da parte delle ditte convenzionate, e corrispondente assistenza durante le operazioni di riparazione;
h) Consulenza agli acquisti informatici e telematici del Comune per una valida gestione;
i) Predisposizione di eventuali convenzioni con soggetti pubblici e privati;
j) Collabora con Responsabili di Settore per la redazione del piano triennale per l'individuazione di misure finalizzate alla razionalizzazione dell'utilizzo delle dotazioni informatiche, nonché della relazione da allegare al consuntivo annuale.

La superiore elencazione ha carattere esemplificativo e non tassativo, rimanendo fermi il diritto-dovere del SIC di svolgere ogni altra funzione necessaria al corretto funzionamento del Sistema Informatico Comunale.

Art. 3 – RESPONSABILE DEL SISTEMA INFORMATICO COMUNALE

Il Responsabile del SIC viene nominato dal Sindaco così come previsto dall'art. 61 punto g) del Regolamento sull'ordinamento degli uffici e dei servizi.

Art. 4 – ACCESSO ALLA RETE

Hanno diritto ad accedere alla rete i dipendenti, gli Amministratori, le ditte fornitrici di software per motivi di manutenzione e limitatamente alle applicazioni di loro competenza, gli enti esterni autorizzati da apposite convenzioni o intese all'accesso alle specifiche banche dati oggetto delle convenzioni e con le modalità stabilite dalle stesse, i collaboratori esterni impegnati nelle attività istituzionali per il periodo di collaborazione.

Il SIC può disporre il divieto di accesso alla rete di determinate risorse informatiche, quando questo è richiesto da ragioni tecniche.

L'accesso agli applicativi è consentito agli utenti che, per motivi di servizio, ne devono fare uso.

Art. 5 - UTILIZZO DELLA RETE

Le risorse informatiche del Comune sono destinate alla informatizzazione dei Servizi e possono essere utilizzate esclusivamente per le attività istituzionali dell'Ente.

E', pertanto, fatto divieto assoluto di utilizzare il SIC per lo svolgimento di:

a) attività che possono rappresentare una violazione della legge in materia di Copyright, fra le quali la copia non autorizzata di software;
b) attività che compromettono in qualsiasi modo la sicurezza delle risorse informatiche;
c) attività illegali;
d) ogni altra attività commerciali non prevista dal contratto di lavoro;.

Le risorse hardware (personal computer, stampanti , server di rete, ecc.) 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, cioè cartelle rese disponibili sotto forma di unità logiche a tutte le postazioni del Settore stesso. Il Responsabile di Settore provvede a comunicare al SIC i livelli di accesso e relative possibilità di utilizzo per ogni singolo utente, nonché eventuali necessità che dovessero presentarsi.

Poichè 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 dovranno riversare (salvare) su dette cartelle:

1) 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;
2) quei dati per cui si rende auspicabile la possibilità di un accesso condiviso da parte di soggetti e/o postazioni diverse, eliminando, in tal modo, la necessità di spostamento fisico mediante supporti esterni;
3) 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. 6 - 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 assolutamente vietato:

1) cablare o collegare apparecchiature alle prese di rete senza l'autorizzazione del Responsabile S.I.C.;
2) utilizzare indirizzi di rete e nomi non espressamente assegnati all'utente dal Responsabile S.I.C.;
3) installare modem configurati per l' accesso remoto;
4) intraprendere azioni allo scopo di degradare le risorse del sistema,
5) consentire ad utenti non autorizzati l'accesso alle risorse,
6) ottenere risorse superiori a quelle già allocate ed autorizzate,
7) accedere a risorse informatiche, sia dell'Ente che di terze parti, violandone le misure di sicurezza;
8) effettuare copie di file di configurazione del sistema.
9) qualsiasi modifica alle impostazioni, connessioni o condivisioni create dal S.I.C.

Art. 7 – PASSWORD

Il S.I.C. provvederà ad attribuire per ogni personal computer una password di accesso alla risorsa stessa, provvederà , inoltre, ad attribuire ad ogni utente autorizzato:

1. login e password di accesso alla rete ,
2. login e password di accesso al software applicativo di pertinenza.

Le suddette password dovranno avere le seguenti caratteristiche: essere cambiate dall'utente utilizzatore della risorsa informatiche con le seguenti disposizioni:

a) devono avere almeno 8 caratteri composte da lettere maiuscole e minuscole, numeri e caratteri speciali . & ^ % $ #;
b) non dovranno essere utilizzate parole del dizionario (qualunque lingua!), nomi propri o geografici;
c) dovranno essere modificate dall'utente utilizzatore al massimo ogni tre mesi.

Qualora il S.I.C., nel corso dell'attività di monitoraggio, verificasse che l'accesso alla rete, nonché agli applicativi, da parte di utenti autorizzati, mediante l'utilizzo di identificativi diversi da quelli agli stessi assegnati, provvederà immediatamente e per iscritto a darne comunicazione al Responsabile di Settore 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 computer 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.

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 (Bloccato su sistemi Xp o con screen-sever protetto da password su sistemi Windows 98).

Art. 8 - 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.

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. 9 – ATTIVITA' VIETATE

Si intende per attività vietata qualsiasi violazione del presente regolamento e di altre norme civili, penali e amministrative che disciplinano le attività e i servizi svolti sulla rete.

In particolare è vietato:

1) Usare la rete in modo difforme da quanto previsto dal presente regolamento.
2) Usare la rete in modo difforme da quanto previsto dalle leggi penali, civili e amministrative.
3) Utilizzare la rete per scopi incompatibili con l'attività istituzionale del Comune di Floridia.
4) Utilizzare login e password a cui non si è autorizzati.
5) Conseguire l'accesso non autorizzato a risorse di rete interne o esterne al Comune di Floridia.
6) Violare la riservatezza di altri utenti o di terzi.
7) Agire deliberatamente con attività che influenzino negativamente la regolare operatività della rete e ne restringano l'utilizzabilità e le prestazioni per altri utenti.
8) Agire deliberatamente con attività che distraggano risorse (persone, capacità, elaboratori).
9) Provocare trasferimenti non autorizzati di informazioni (software, basi dati, ecc).
10) Installare o eseguire deliberatamente o diffondere su qualunque computer e sulla rete, programmi destinati a danneggiare o sovraccaricare i sistemi o la rete; sono compresi a titolo esemplificativo virus, cavalli di troia, worms, spamming della posta elettronica.
11) Installare o eseguire deliberatamente programmi software non autorizzati e non compatibili con l'attività istituzionale.
12) Cancellare, copiare o asportare deliberatamente programmi software per scopi personali.
13) Installare deliberatamente componenti hardware non compatibili con l'attività istituzionale.
14) Rimuovere, danneggiare deliberatamente o asportare componenti hardware.
15) Utilizzare le risorse hardware e software e i servizi disponibili per scopi personali.
16) Utilizzare la posta elettronica con la parola chiave di altri utilizzatori.
17) Utilizzare la posta elettronica inviando e ricevendo materiale che violi le leggi.
18) Utilizzare l'accesso a Internet per scopi personali.
19) Se non espressamente autorizzati e per particolari motivi tecnici, accedere direttamente a Internet con modem collegato al proprio posto di lavoro, senza utilizzare la connessione autorizzata tramite LAN.
20) Connettersi ad altre reti senza autorizzazione.

21) Monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività degli utenti, leggere, copiare o cancellare files e software di altri utenti, senza averne l'autorizzazione esplicita.
22) Usare l'anonimato o servirsi di risorse che consentano di restare anonimi.

Art. 10 - 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.

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 segnalarlo al SIC con la massima urgenza.

Del programma "antivirus" vengono fornite, regolarmente e con cadenza giornaliera, versioni aggiornate, per consentire la massima sicurezza.

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.

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. 11 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 i protocolli di sicurezza.

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 client/server e 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.

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

Tutti i Responsabili di Settore, attraverso i propri collaboratori, dovranno concordare con il Responsabile del Sistema Informatico Comunale come inserire tutti gli atti prodotti (delibere, determine, regolamenti, comunicati stampa, bandi di gara, avvenimenti vari, ecc.) per un costante aggiornamento del sito del Comune di Floridia.

Art. 12 - DOTAZIONE SOFTWARE

Ogni personal computer e, più in generale, ogni attrezzatura informatica, ha in dotazione software di utilità forniti su rilascio di 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 dal Responsabile di Settore e dall'utente assegnatario, per ogni singola attrezzatura, indicante le caratteristiche della stessa (marca, modello, numero di matricola, 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' 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 segnalare, in forma scritta, al Responsabile del Settore, per i provvedimenti anche disciplinari del caso, ogni eventuale installazione non registrata.

Per quanto sopra esposto, il SIC è tenuto ad effettuare periodici controlli su ogni postazione di lavoro e a segnalare in forma scritta, al Responsabile del Settore, eventuali inadempienze.

Art 13 – 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 del SIC.

Art. 14 - 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.

Art.15 - NORME DI CHIUSURA

Per quanto sopra il Comune provvede a:

- acquisire, predisporre e gestire apparecchiature informatiche e telematiche;
- fornire un articolato e qualificato servizio di consulenza;

- organizzare corsi di formazione, seminari e incontri, avvalendosi della collaborazione di esperti anche esterni al Comune;
- definire le politiche di sicurezza e a far rispettare il regolamento informatico.