REGOLAMENTO PER L'UTILIZZO DELLE RISORSE INFORMATICHE E DI RETE
Approvato con D.G.C. n. 54 del 29.03.2006

INDICE:

Art. 1 - Motivazioni

Negli ultimi anni le risorse informatiche all'interno dell'Ente sono molto aumentate e con esse l'utilizzo della rete Internet. Tutto questo ha avuto importanti ricadute sui problemi della sicurezza.
Si rende quindi necessario attivare una serie di norme, restrizioni e controlli per garantire la sicurezza dei sistemi e definire le responsabilità degli utilizzatori delle risorse.
L'adozione di queste politiche è prevista nell'intento di:
F) Garantire la massima efficienza delle risorse informatiche e del loro utilizzo.
G) Garantire la riservatezza delle informazioni e dei dati.
H) Assicurare la continuità del servizio nell'interesse dell'Ente e dei Cittadini.
I) Garantire il rispetto delle leggi in materia di utilizzo delle risorse informatiche.
J) Garantire la massima sicurezza nell'interazione tra il Comune di Noale e le altre istituzioni.

In questa prospettiva è compito dell'Ente:
1) Adottare tutti i dispositivi di sicurezza necessari a difendere i propri sistemi informatici.
2) Implementare meccanismi di controllo e monitoraggio, sia "hardware", sia "software", e sia normativi, capaci di evitare intrusioni e/o abusi.
3) Responsabilizzare e formare gli utenti circa i rischi penali, civili, amministrativi connessi all'uso indebito dei mezzi informatici.
4) Adottare tecniche atte ad evitare che i propri utenti, utilizzando gli strumenti informatici dell'Ente, compiano abusi legati all'utilizzo improprio delle risorse messe a disposizione, e in particolare abusi legati all'uso della rete Internet.

Art. 2 - Introduzione

Il Servizio Informativo ed Informatico dell'Ente (di seguito indicato anche come Servizio Informatica) si occupa della configurazione e dell'amministrazione delle risorse informatiche, delle reti informatiche usate internamente all'ente e dell'interfaccia di accesso alle reti esterne.
Per risorse informatiche si intendono:
a) Macchine centrali con funzioni di "server" degli applicativi e di "file server"
b) Personal computer, computer portatili, stampanti e altri strumenti utilizzati dai dipendenti, dagli amministratori, e dalle altre figure operanti nell'Ente, con incarichi professionali, stagisti, tirocinanti ed eventuali ospiti.
c) Apparati di rete.
d) Tutto il software e i dati contenuti negli archivi informatici necessari al funzionamento dell' Ente.

Art. 3 - Regole di utilizzo della rete aziendale e di internet

Premessa:
Utenti della rete sono tutti coloro che per scopo professionale, o comunque connesso alle attività dell'Ente, fanno uso abituale od occasionale delle risorse informatiche di cui sopra, e quindi sono tali: i dipendenti, gli amministratori, il personale con incarichi professionali, gli stagisti e i tirocinanti, gli eventuali ospiti istituzionali.
Sono altresì utenti della rete i cittadini che usufruiscono del servizio di accesso ad Internet offerto dalla Biblioteca Comunale, e, in forma diversa, i visitatori del sito istituzionale, qualora questo sia collegato in forma automatica alle banche dati dell'Ente. Queste ultime due categorie di utilizzatori, tuttavia, sono qui citate per completezza ma non sono direttamente soggette al presente regolamento.
Le seguenti regole devono essere seguite attentamente da tutti gli utenti della Rete aziendale. Per quanto non specificato nel presente documento è richiesto comunque un atteggiamento ispirato alla correttezza ed alla buona fede; resta valida in ogni caso l'assunzione di responsabilità personale per il proprio PC; in caso di dubbi, necessità di informazioni, sospetto di tentativi di intrusione ecc. l'utente deve rivolgersi immediatamente al Servizio Informatica.

Art. 4 - Accesso alle risorse della Rete aziendale

L'accesso alle risorse della Rete aziendale è riservato agli utenti;
Ogni risorsa informatica collegata alla Rete è affidata ad un utente.
Qualora l'utente debba accedere a Internet tramite la rete dell'Ente, è tenuto a sottoscrivere la dichiarazione di assunzione di responsabilità e acquisisce lo status di responsabile per la gestione e l'utilizzo della risorsa stessa sulla rete;
Il Settore Informatica potrà accedere alla risorsa informatica dell'utente per compiti di monitoraggio, controllo e/o aggiornamenti, ai fini della sicurezza del sistema e della rete, nel rispetto della presente politica di gestione e della riservatezza dei dati personali (ai sensi del T.U. 196 / 2003), sentito il Dirigente responsabile.

Art. 5 - Utilizzo delle risorse informatiche e reti

Le risorse informatiche dell'Ente possono essere utilizzate esclusivamente per le attività istituzionali. Non è consentito l'uso per fini personali.
In particolare, e al solo fine di memoria, si ricorda che sono tassativamente vietate e perseguibili amministrativamente, civilmente ed in taluni casi, anche penalmente le seguenti attività:
- Accedere a siti ed¬ acquisire o comunque diffondere prodotti informativi lesivi del comune senso del pudore.
- Diffondere prodotti informativi lesivi dell'onorabilità,¬ individuale o collettiva.
- Diffondere prodotti informativi di propaganda¬ politica.
- Diffondere, in rete o con qualsiasi altro mezzo di¬ comunicazione, informazioni riservate di qualunque natura.
- Svolgere ogni¬ tipo di attività commerciale.
- Compiere attività che possono rappresentare¬ una violazione della legge in materia di Copyright, fra le quali la copia non autorizzata di software, CD audio e video, clonazione o programmazione di smart card.
- Compiere attività che compromettono in qualsiasi modo la sicurezza¬ delle risorse informatiche e della rete aziendale.
- Ogni altra attività¬ illegale qui non elencata.

L'Ente provvede a disporre opportuni dispositivi di monitoraggio del traffico sulla rete, nel rispetto delle vigenti leggi sulla riservatezza personale, che consentano di evidenziare e rintracciare eventuali anomalie ed abusi.
L'Ente si riserva, inoltre, a norma di legge, di predisporre, se del caso, idonei dispositivi di filtro per limitare l'accesso ai siti non autorizzati.

Art. 6 - Responsabilità degli utenti

L'utente non può in alcun caso modificare la configurazione di rete e non può effettuare manomissioni o interventi sulle apparecchiature o sui programmi non formalmente autorizzati dal servizio tecnico del Servizio Informatica, al quale deve comunicare tempestivamente le necessità di interventi su apparecchiature e programmi in ordine alla corretta prestazione dei servizi;
L'accesso alla risorsa informatica è personale e vi si accede tramite nome utente e/o password di identificazione. L'accesso non può essere condiviso o ceduto.
Gli utenti sono responsabili per la protezione dei dati utilizzati e/o memorizzati nei sistemi in cui hanno accesso; è fatto loro divieto di accedere direttamente o indirettamente a directory, files e servizi al cui uso non sono stati autorizzati.
La password è personale e non cedibile o trasmissibile a terzi: è fatto divieto a ciascun utente di divulgare, per fatto imputabile a lui direttamente o indirettamente, password, login e comunque chiavi di accesso riservate. Se smarrite, va fatta immediata segnalazione e richiesta di sostituzione al servizio informatica.
Gli utenti sono tenuti a non lasciare incustoditi o accessibili gli strumenti elettronici mentre è in corso una sessione di lavoro.
Gli utenti sono obbligati a segnalare immediatamente al Servizio Informatica ogni sospetto di effrazione, incidente, abuso o violazione della sicurezza; gli utenti sono tenuti a mantenersi aggiornati, controllando periodicamente le direttive del Servizio Informatica divulgate tramite e-mail o rete intranet.
Nell'interscambio di documenti gli utenti sono tenuti, a seconda del destinatario, ad utilizzare i formati non modificabili o modificabili ma privi di informazioni aggiuntive attinenti all'Ente: rispettivamente ".PDF (firmato)" e ".RTF".

Art. 7 - Archiviazione di sicurezza dei dati (BackUp)

L'utente è responsabile della conservazione dei dati necessari alla propria attività istituzionale e contenuti nella memoria di massa del computer affidatogli.
A questo scopo, tramite la connessione di rete, effettua periodicamente il salvataggio dei propri archivi, verso le aree predisposte sui "server".
E' compito del Settore Informatica predisporre il salvataggio su idoneo mezzo rimovibile delle suddette aree di immagazzinamento dei dati sui server.

Va effettuata copia di tutti i dati e i documenti generati nel corso della propria attività lavorativa, che siano in qualunque modo rilevanti per gli scopi istituzionali dell' Ente. I documenti e i dati che siano ritenuti di non immediata necessità o utilizzo devono essere raccolti in archivi opportunamente denominati e fatti oggetto di salvataggio fuori linea, normalmente su mezzo ottico, ed archiviati in luogo protetto. Le attività di salvataggio fuori linea, di tali contenuti, sono demandate alla responsabilità delle diverse aree, il Settore Informatica si occupa unicamente di predisporre gli strumenti e attivarsi per garantire la formazione tecnologica agli utenti.

Art. 8 - Software e copyright

L'utente risponde del software installato sul computer che gli è affidato.
Il Servizio informatica provvede all'acquisto delle licenze necessarie per il software presente sui computer dell'Ente.
E' vietato distribuire indebitamente, all'interno o all'esterno dell' Ente il software, soggetto a Copyright, acquistato dall'Ente, al di fuori dei termini delle licenze.

Art. 9 - Le seguenti attività sono tassativamente vietate:

Utilizzare strumenti che potenzialmente sono in grado di¬ consentire l'accesso non autorizzato

alle risorse informatiche (ad esempio cracker, programmi di condivisione di file e programmi di “chat” quali IRC, ICQ, WinMx, o software di monitoraggio della rete in genere).
Riconfigurare¬ arbitrariamente i servizi già messi a disposizione in modo centralizzato, quali DNS , DHCP o server internet (Web o E-mail).
Intercettare pacchetti sulla¬ rete, utilizzare sniffer o software di analisi del traffico (Spyware) dedicati a carpire dati personali, password e ID degli utenti o a controllare in qualunque modo le attività di rete.
Installare programmi ricavati da dischetti¬ ricevuti da terzi o allegati a riviste o scaricati dalla rete, anche se di tipo gratuito “freeware” o “shareware”, se non previa autorizzazione del proprio Dirigente e sentito il Servizio Informatica.

Art. 10 – Responsabile della sicurezza

Il Responsabile della Sicurezza è il soggetto a cui è conferito il compito di sovraintendere a una o più risorse informatiche dell’Ente (art.29 Dlgs.196/2003)
Lo stesso è obbligato ad operare nel rispetto delle politiche dell’Ente in materia di sicurezza, a garantire la massima riservatezza nella trattazione dei dati personali anche desunti dal software di analisi del traffico, a mantenere riservate le informazioni relative al collegamento degli utenti fatti salvi i casi di interessamento della Magistratura a fronte di ipotesi di reato; può fornire ai funzionari/dirigenti delle Aree i report contenenti dati aggregati relativi all'andamento del traffico, ai picchi anomali settoriali, alla statistica generale di accesso ai siti più frequentati.
Il Servizio Informatica revoca l'accesso temporaneo alla risorsa informatica e di rete, sentito il Dirigente preposto, qualora questo sia utilizzato impropriamente o in violazione delle leggi vigenti.
Potrà altresì interrompere temporaneamente la prestazione del servizio in presenza di motivati problemi di sicurezza, riservatezza o guasto tecnico, dandone tempestiva comunicazione all'utente.
Il personale del Servizio informatica può accedere in qualsiasi momento, anche senza preavviso, ai locali e alle risorse informatiche dell’Ente sia in caso di emergenza, sia per effettuare gli interventi di assistenza, verifica e supporto.