



**AZIENDA PUBBLICA DI SERVIZI ALLA PERSONA  
"G. CHIABA"  
SAN GIORGIO DI NOGARO**

**APPROVATO CON DELIBERAZIONE DEL C. di A. N. 12 DEL 06/03/2008**

**REGOLAMENTO PER L'UTILIZZO DI COMPUTER E RETI DI  
TRASMISSIONE DATI**

**Art. 1 – OGGETTO E FINALITÀ**

1. Il presente Regolamento fornisce le regole principali per un corretto uso delle risorse informatiche dell'Azienda Pubblica di Servizi alla Persona "G. Chiabà", di seguito denominata Azienda.
2. Gli elaboratori e la rete di trasmissione dati costituiscono strumenti indispensabili per l'Azienda, in quanto consentono l'accesso, l'elaborazione e la distribuzione dell'informazione e della conoscenza sviluppate all'interno ed all'esterno di essa. L'Azienda pertanto concede in uso al personale e ai collaboratori le proprie apparecchiature informatiche e ne promuove l'utilizzo, ritenendole strategiche per le proprie attività istituzionali.
3. Poiché tali tecnologie potenziano la capacità individuale all'accesso, alla copia, all'analisi ed alla rielaborazione delle informazioni, gli utenti devono comunque essere coscienti dei limiti che ne configurano un uso appropriato, in particolare per quanto riguarda il rispetto degli altrui diritti alla privacy, della proprietà intellettuale e degli altri diritti ed obblighi conseguenti.
4. Gli utenti della rete e delle risorse di elaborazione dell'Azienda sono tenuti a farne uso corretto, ad averne cura ed a rispettare i diritti sopra citati, osservando nello specifico le regole stabilite nel presente Regolamento.
5. L'Azienda si impegna a dimensionare opportunamente le risorse informatiche e di rete disponibili in funzione delle necessità e priorità dell'utenza.

**Art. 2 - AMBITO ED APPLICABILITÀ DEL REGOLAMENTO**

Il presente Regolamento si applica a tutto il personale e collaboratori esterni, ai volontari che operano per conto dell'Azienda ai quali, a qualsiasi titolo, sia concesso l'uso delle risorse informatiche dell'Azienda, sia controllate individualmente che condivise, gestite su un singolo computer o rese disponibili in rete. Si applica a tutte le attrezzature di elaborazione e comunicazione possedute o detenute a qualsiasi titolo dall'Azienda.

**Art. 3 – ATTIVITA' NON CONSENTITE NELL'USO DELLA RETE**

Nell'uso della Rete Informatica non sono consentite le seguenti attività:

- ✓ Utilizzare la Rete in modo difforme da quanto previsto dal presente regolamento.

- ✓ Utilizzare la Rete per scopi incompatibili con l'attività istituzionale dell'Azienda.
- ✓ Comunicare ad altri, o comunque rendere disponibili ad altri, i dati relativi al proprio account di rete (username e password). La password è segreta, strettamente personale, non deve essere divulgata e deve essere debitamente conservata.
- ✓ Conseguire l'accesso non autorizzato a risorse di rete esterne alla Rete Aziendale, tramite la stessa Rete Informatica Aziendale.
- ✓ 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, spamming della posta elettronica).
- ✓ Installare o eseguire programmi software non autorizzati o non compatibili con l'attività istituzionale.
- ✓ Cancellare, copiare o asportare programmi software per scopi personali.
- ✓ Installare componenti hardware non compatibili con l'attività istituzionale.
- ✓ Installare componenti hardware non acquistati dall'Azienda e non di proprietà della stessa e non autorizzati.
- ✓ Rimuovere, danneggiare o asportare componenti hardware.
- ✓ 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 rivolti alla violazione della sicurezza del sistema e della privacy.
- ✓ Usare l'anonimato o servirsi di risorse che consentano di restare anonimi.
- ✓ Abbandonare il posto di lavoro lasciandolo senza protezione da accessi non autorizzati.

#### **ART. 4 - ATTIVITA' NON CONSENTITE NELL'UTILIZZO DI INTERNET E DELLA POSTA ELETTRONICA**

Nell'utilizzo di Internet e della Posta Elettronica non sono consentite le seguenti attività:

- ✓ per scopi personali;
- ✓ L'accesso a siti inappropriati (esempio siti pornografici, di intrattenimento, ecc.).
- ✓ Lo scaricamento (download) di software e di file non necessari all'attività istituzionale.
- ✓ 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).
- ✓ 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 (D.lgs. 196 del 30/6/2003).
- ✓ Un uso che possa in qualche modo recare qualsiasi danno all'Azienda o a terzi.
- ✓ L'apertura di allegati ai messaggi di posta elettronica senza il previo accertamento dell'identità del mittente.
- ✓ Inviare tramite posta elettronica user-id, password, configurazioni della rete interna, indirizzi e nomi dei sistemi informatici.

## **ART. 5 - UTILIZZO DELLE STAMPANTI E DEI MATERIALI DI CONSUMO**

L'utilizzo delle stampanti e dei materiali di consumo in genere (carta, inchiostro, toner, floppy disk, supporti digitali come CD e DVD) è riservato esclusivamente ai compiti di natura strettamente istituzionale.

Devono essere evitati in ogni modo sprechi dei suddetti materiali o utilizzi eccessivi.

## **Art. 6 - FIGURE E RESPONSABILITÀ DELL'AMMINISTRATORE RESPONSABILE DI RETE**

1. Il Titolare dell'Azienda, identificato nella figura del Presidente, è responsabile di fronte alla legge di tutti i computer, gli apparati di rete e le reti acquistate od affittate dall'Azienda.

2. Il controllo e la supervisione di ogni particolare sistema è delegato al responsabile dell'Azienda, identificato nella figura del Direttore Generale.

Per le attrezzature possedute o detenute dall'Azienda, tale soggetto è definito **amministratore responsabile di rete** ai fini del presente Regolamento.

3. L'amministratore responsabile di rete può delegare altre persone ad amministrare il sistema, definite **amministratori di sistema**.

## **Art. 7 - AMMINISTRATORE DI SISTEMA**

1. L'attività dell'amministratore di sistema può inquadrarsi in due contesti complementari:

a) **Attività di ordinaria amministrazione** - Volta a garantire il normale funzionamento e lo sviluppo dei sistemi amministrati. In tal caso l'amministratore di sistema opera di concerto con l'utente, e comunque coordinandosi in via preventiva con l'amministratore responsabile di rete.

b) **Gestione delle emergenze** - Quando si rilevino condizioni che pongano a rischio immediato la corretta funzionalità dei sistemi o della rete, o la sicurezza dei dati e dei sistemi, l'amministratore di sistema può operare in autonomia o mediante il supporto delle ditte esterne alle quale viene affidato l'incarico di manutenzione dei sistemi installati presso l'Azienda. Immediatamente dopo l'intervento, se importante, è tenuto a segnalare per iscritto agli utenti coinvolti e all'amministratore responsabile di rete i dettagli dell'evenienza occorsa.

2. L'amministratore di sistema deve avere ragionevole cura:

a) nel prendere precauzioni contro i furti ed i danni ai componenti del sistema;

b) nell'attuare rigorosamente tutti gli accordi di licenza hardware e software applicabili al sistema;

c) nel trattare informazioni riguardanti gli utenti del sistema, nonché le informazioni depositate nel sistema dagli utenti medesimi, in modo appropriato, applicando rigorosamente le norme e le pratiche atte a garantire la sicurezza dei sistemi, delle reti e dei dati. Si fa particolare riferimento al caso di azioni dolose volte a violare l'integrità dei sistemi, dei dati o della privacy (ad es. intrusioni, diffusioni di virus, etc.), ed al caso di incidenti di natura tecnica (ad es. incendio, perdita di dati, etc.);

d) nel diffondere informazioni sui regolamenti e le procedure specifiche che regolano l'accesso e l'uso del sistema, sui servizi forniti e su quelli esplicitamente non forniti. Un documento scritto consegnato agli utenti sarà considerato una notifica adeguata;

3. Un amministratore di sistema può temporaneamente interdire l'accesso e l'uso delle risorse informatiche ad un utente se, sulla base di comprovati motivi, lo ritiene necessario per garantire la sicurezza del sistema o della rete. Se l'amministratore di sistema ha chiare evidenze di cattivo uso delle risorse informatiche che indirizzino ad attività di elaborazione o files di uno specifico individuo, deve attuare uno o più dei seguenti passi, considerati appropriati per la protezione degli altri utenti, della rete e dei sistemi di computer:

a) notificare per iscritto le eventuali indagini all'Amministratore Responsabile di rete;

b) adottare tutti i provvedimenti e le azioni ritenute necessarie e/o opportune dal responsabile di cui al punto a), per inibire il propagarsi dei danni alle risorse di rete.

### **Art. 8 – VIOLAZIONI AL PRESENTE REGOLAMENTO**

Gli utenti che non osservano le regole contenute nel presente regolamento saranno soggetti alle sanzioni previste dalla normativa vigente.

**Si allegano al presente regolamento, quale parte integrante e sostanziale:**

- ✓ **allegato n. 1: linee guida per la protezione dei personal computer portatili;**
- ✓ **allegato n. 2: linee guida per la sicurezza dell'informazione, ad uso degli incaricati del trattamento dati.**