



PROT. N. ....

FROSINONE, 2 FEB 2007

# REGOLAMENTO RELATIVO ALL'UTILIZZO DEI SISTEMI INFORMATICI E TELEMATICI AZIENDALI DELL'A.T.E.R. DELLA PROVINCIA DI FROSINONE

## 1. Scopo - Definizioni - Ambito di Applicazione

Il presente Regolamento disciplina le modalità di utilizzo delle Risorse Informatiche dell'azienda ATER della provincia di Frosinone.

Per Risorse Informatiche si intendono:

- le apparecchiature informatiche (HARDWARE): server, router, firewall, personal computer, stampanti, plotter, scanner, fax di rete, fotocopiatrici di rete e tutte le apparecchiature in grado di collegarsi alla rete aziendale anche in modalità senza fili (wireless);
- i programmi informatici (SOFTWARE): sistemi operativi (Windows, Linux, ecc.), applicazioni informatizzate (Gelim-Gepat, ecc.), programmi di utilità (Acrobat Reader, WinZip, ecc.), prodotti per l'Office Automation (Word, Excel, Access, ecc.);
- le informazioni della banca dati aziendale compresi tutti i documenti prodotti con le suddette attrezzature;
- L'accesso alle informazioni sulla Rete Locale (Intranet)
- L'accesso alle informazioni sulla Rete Esterna (Internet);
- Le informazioni del sito Web della Rete Intranet e della Rete Internet;
- La posta elettronica (e-mail).

Il presente Regolamento si applica a tutti gli Utilizzatori Interni e Esterni autorizzati ad accedere alle Risorse Informatiche dell'ATER.

## 2. Principi Generali - Diritti - Responsabilità

L'ATER promuove l'utilizzo delle Risorse Informatiche quali strumenti utili a perseguire le proprie finalità istituzionali.

L'ATER si impegna a dare a tutti gli Utilizzatori gli strumenti necessari, apparecchiature e informazioni, -Hardware e Software-, per essere più efficienti ed efficaci nell'azione tecnico-amministrativa istituzionale.

Ogni Utilizzatore è personalmente responsabile del corretto uso delle Risorse Informatiche alle quali ha accesso e si impegna a trattarle con senso di responsabilità e cura al fine di evitare perdite, furti o danni. Le Risorse Informatiche devono essere utilizzate soltanto per scopi legati alle attività professionali di ciascun Utilizzatore, attinenti alle proprie mansioni e inerenti alle attività istituzionali aziendali.



Le Vigenti Normative che governano "la protezione dei dati personali", "il diritto d'autore", "la tutela del software e le licenze d'uso", "la diffamazione", "la discriminazione" si applicano anche nel campo informatico e telematico.

I programmi informatici (software) sono stati equiparati a "beni" e sono soggetti a tutte le leggi che proteggono i "beni materiali", quali ad esempio il furto, l'appropriazione indebita, la truffa e la ricettazione.

Le apparecchiature informatiche (hardware) sono state equiparate a "luoghi" e sono soggetti a tutte le leggi che proteggono i luoghi fisici e la proprietà pubblica e privata, quali ad esempio la violazione di domicilio, l'attentato a impianti di pubblica attività, e interruzione di pubblico servizio.

Tutti gli Utilizzatori hanno l'obbligo di riferire ogni sospetta o accertata violazione delle Vigenti Normative o delle regole di comportamento indicate nel presente Regolamento.

### **3. Amministrazione delle Risorse Informatiche - Responsabilità**

Il Responsabile del Servizio Informatico, è l'unico soggetto a cui è conferito il compito di sovrintendere alle Risorse Informatiche dell'ATER ed espleta in maniera esclusiva, ai soli fini della sicurezza informatica, dell'integrità, della disponibilità e della protezione dei dati, nel pieno rispetto dei diritti dei lavoratori, le seguenti attività:

- gestire tutte le Risorse Informatiche dell'ATER collegate in rete o meno;
- gestire le Credenziali di Accesso degli Utilizzatori secondo quanto stabilito da ogni Dirigente di Riferimento;
- monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare il corretto utilizzo delle Risorse Informatiche;
- adottare tutte le misure protettive nei confronti degli attacchi da parte di programmi malevoli (Virus) attivando i più recenti software Antivirus
- proteggere le Risorse Informatiche da intrusioni esterne indesiderate o non autorizzate o fraudolente, tramite opportune configurazioni di router e firewall e l'utilizzo della cifratura nella trasmissione dei dati.
- rimuovere o installare Componenti Hardware;
- rimuovere o installare Programmi Software;
- utilizzare le Credenziali di Accesso di Amministratore di Sistema o di un Utilizzatore per accedere alle informazioni presenti su una risorsa assegnata, nel caso di prolungata assenza o irrintracciabilità o impedimento dello stesso, per attività indifferibili richieste esplicitamente dal Dirigente di Riferimento e comunque limitate al tempo strettamente necessario per il compimento delle attività;
- effettuare periodicamente le copie di sicurezza dei dati e a conservarle in luogo sicuro e protetto ma velocemente reperibili in caso di necessità;
- adottare le strategie alternative (Disaster Recovery), in caso di prolungato ammanco del Sistema Informativo.

Per l'immagine dell'ATER su Internet e sulla Intranet è responsabile la Direzione Generale che stabilisce le necessarie regole e in particolare quali pagine di accesso devono essere create in modo uniforme.



Il realizzatore della pagina Web (Webmaster) è colui che trasferisce sulla rete le informazioni trasmesse dal responsabile di riferimento, impegnandosi ad aggiornare frequentemente il sito Web, e adottando tutte le misure necessarie ad impedire accessi non autorizzati e manipolazioni delle pagine realizzate.

#### **4. Sicurezza - Modalità di Accesso**

Il Responsabile del Servizio Informatico usa tutte le proprie capacità e le proprie competenze per adottare tutte le misure minime necessarie e sufficienti per consentire la protezione delle Risorse Informatiche, per prevenire, accertare ed eliminare tutti i difetti di sicurezza e rimuovere eventuali difetti tecnici.

Assegna a ciascun Utilizzatore un profilo con le credenziali di accesso (Account) alle Risorse Informatiche, composta da un Nome Utente (User Name) e da una Parola d'Ordine (Password) che, in ottemperanza alle Vigenti Normative, dovrà possedere i requisiti di complessità relativi alla lunghezza minima consentita, al periodo minimo di validità, al numero minimo e al tipo dei caratteri speciali da utilizzare.

Ogni Utilizzatore deve contribuire alla sicurezza complessiva delle Risorse Informatiche in particolare deve:

- applicare le norme di sicurezza decise dal Servizio Informatico;
- assicurare la protezione del proprio Account (User Name e Password), a tenerlo segreto, a non divulgarlo e a cambiarlo al primo sospetto di violazione;
- bloccare il collegamento alle Risorse Informatiche, prima di abbandonare, anche se brevemente, il proprio posto di lavoro;
- segnalare ogni tentativo di violazione del proprio Account e le eventuali anomalie.
- evitare, senza l'esplicita approvazione del Servizio Informatico, l'installazione di software, l'aggiunta o la rimozione di parti di hardware che possano provocare danno alle Risorse Informatiche o che ne compromettano il buon funzionamento.

#### **5. Utilizzo delle Stampanti e dei Materiali di Consumo**

L'utilizzo delle stampanti e dei materiali di consumo (carta inchiostro, toner, floppy disk, cd, dvd, ecc.) è riservata esclusivamente ai compiti di natura istituzionale.

Devono essere evitati in ogni modo sprechi, abusi e utilizzi eccessivi.

Lo scambio di informazioni tra gli Utilizzatori, per evitare l'eccessivo consumo della carta, deve avvenire prevalentemente, se non esclusivamente, tramite posta elettronica.

#### **6. Utilizzatori - Attività Non Consentite**

L'Utilizzatore è il responsabile dell'integrità, della disponibilità, della protezione e della sicurezza delle proprie Risorse Informatiche il cui utilizzo deve rientrare nelle attività istituzionali dell'ATER e deve essere attinente allo svolgimento delle mansioni assegnate, o



comunque espressamente autorizzate dal Dirigente di Riferimento o dal Responsabile del Servizio Informatico.

Per non interferire volontariamente con il buon funzionamento dei sistemi informatici e telematici, non è consentito:

- installare o utilizzare Software senza disporre delle opportune licenze d'uso o per scopi personali;
- installare o utilizzare componenti Hardware non di proprietà dell'ATER o per scopi personali;
- diffondere Software destinato a danneggiare o a sovraccaricare le Risorse Informatiche;
- modificare le impostazioni e le configurazioni delle proprie Risorse Informatiche;
- utilizzare supporti di qualsiasi tipo di proprietà dell'ATER per scopi personali;
- inserire Password Locali al BIOS se non espressamente autorizzati e dovutamente comunicate al Responsabile del Servizio Informatico.
- utilizzare la connessione Internet dell'ATER per:
  - ascoltare la radio o guardare video o filmati in streaming audio/video;
  - effettuare transazioni finanziarie e bancarie o acquisti on line;
  - scaricare software di prova (shareware) o gratuiti (freeware);
  - effettuare scaricamenti (download) di file di notevoli dimensioni che possano rallentare la velocità e l'ampiezza della banda di Internet;
  - registrarsi a siti per l'uso di "Chat Line", "Forum", "NewsGroup";
  - accedere a siti inappropriati (pornografici, illegali, di intrattenimento, ecc.);
  - utilizzare programmi per la condivisione e lo scambio di file in modalità peer to peer (Napster, Emule, Edonkey, ecc.);
  - per uso personale.
- utilizzare la posta elettronica (e-mail) per:
  - inoltrare "catene" di posta elettronica (catene di S. Antonio e simili) anche se afferenti a presunti problemi di sicurezza;
  - inviare allegati di notevoli dimensioni (oltre i 4 Mbyte);
  - trasmettere dati sensibili, confidenziali e personali ovvero notizie su User Name, Password, configurazioni, indirizzi IP e nomi assegnati alle apparecchiature informatiche;
  - diffondere messaggi oltraggiosi e/o discriminatori per sesso, lingua, religione, razza, origine etnica, opinione o appartenenza sindacale e/o politica
  - inviare arbitrariamente e indiscriminatamente messaggi a gruppi o liste di distribuzione;
  - aprire allegati senza il previo accertamento dell'identità del mittente;
  - uso personale.

Eventuali deroghe alle Attività Non Consentite devono essere espressamente autorizzate dal Dirigente di Riferimento o dal Responsabile del Servizio Informatico.

## **7. Definizione di Abuso - Notifiche - Sanzioni**

Chi accede alle Risorse Informatiche senza la dovuta autorizzazione o ne fa un uso sproporzionato danneggiandone la perfetta efficienza, chi contravviene alle Vigenti Normative in materia di criminalità informatica, chi non rispetta le norme del presente Regolamento, chi detiene, consulta, utilizza materiale dai contenuti pornografici o razzisti, commette un abuso e può essere punito.



Chiunque venga a conoscenza di un abuso ha l'obbligo di informare il Responsabile del Servizio Informatico che può, preventivamente, a protezione della sicurezza delle Risorse Informatiche, qualora lo ritenga necessario, neutralizzare le attività pericolose e sospendere le credenziali di accesso.

I costi derivanti da danni per eventuali abusi accertati, possono essere addebitati a chi li ha causati.

Poiché in caso di violazioni contrattuali e giuridiche, sia l'Azienda, sia il singolo lavoratore sono potenzialmente perseguibili con sanzioni, anche di natura penale, l'Azienda verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole e l'integrità del proprio sistema informatico.

La non osservanza del presente regolamento può comportare sanzioni disciplinari, civili e penali.

## 8. Entrata in Vigore

Il presente Regolamento entrerà in vigore al momento della sua approvazione da parte del Consiglio di Amministrazione e verrà pubblicato sul sito Web della Rete Locale riservata al personale interno.

Servizio Informatico  
Giuliano Crecco