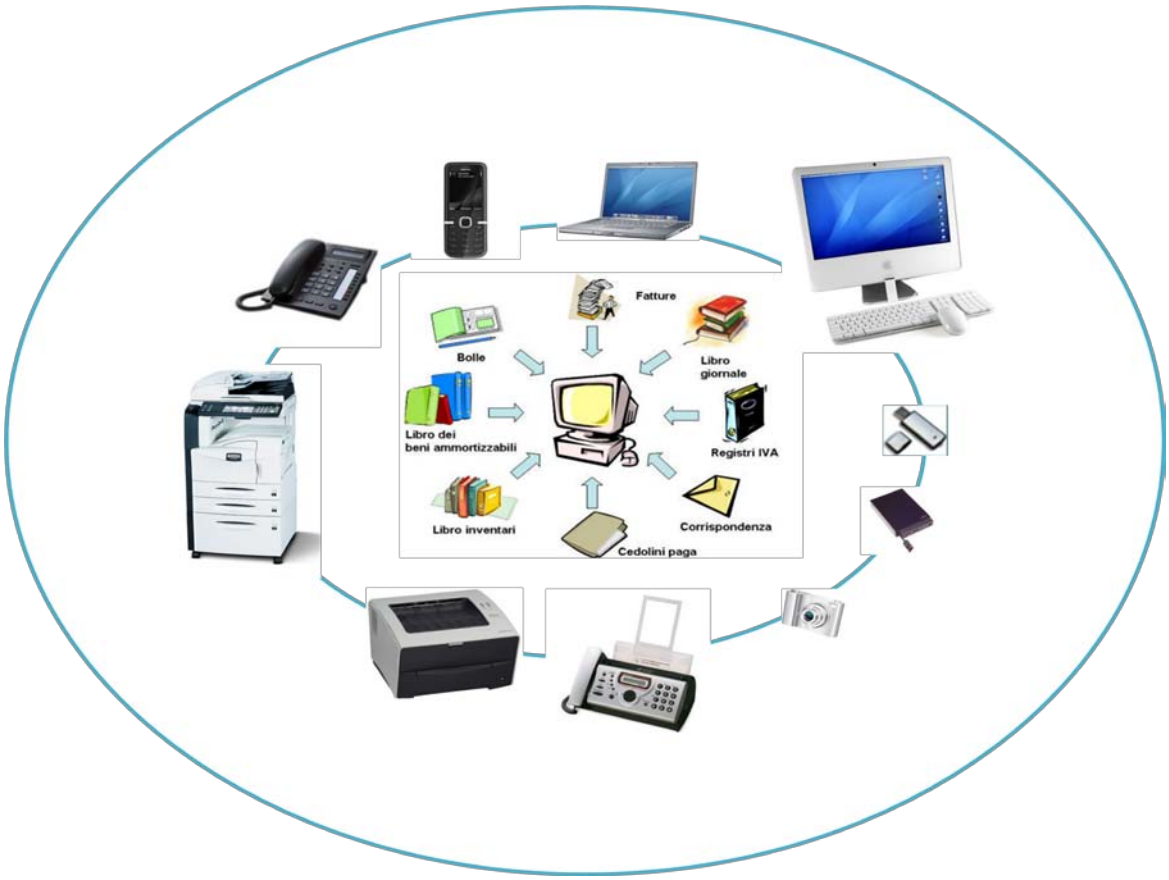
REGOLAMENTO RELATIVO ALL'ACCESSO E ALL'USO DEL SISTEMA INFORMATIVO E TELEMATICO AZIENDALE GESTIONE DEGLI ARCHIVI INFORMATICI E CARTACEI



Approvato con Delibera del CDA n° 35 del 3 giugno 2010

INDICE

In accordo e conformità con Provvedimento del Garante per la protezione dei dati personali 1° marzo 2007
(G.U. n° 58 del 10/3/2007)

Provvedimento del Garante Privacy del 27 novembre 2008
(G.U. n. 300 del 24/12/ 2008)

ART. 1 - OGGETTO E AMBITO DI APPLICAZIONE

1. Il presente Regolamento disciplina le modalità di accesso e di uso della Rete Informatica e Telematica Aziendale e dei servizi che è possibile ricevere o offrire all'interno ed all'esterno ad essa, anche con la finalità di garantire la sicurezza di tutte le informazioni residenti negli archivi collegati di proprietà del Comune di Parma.

2. La Rete è costituita dall'insieme delle risorse informatiche e telematiche infrastrutturali e dal patrimonio informativo digitale.

3. Le Risorse infrastrutturali sono le componenti hardware (computer, video, ecc.) e software (sistema operativo, programmi, ecc.), gli apparati elettronici collegati alla Rete Informatica e gli apparecchi telematici.

4. Il Patrimonio informativo è l'insieme delle banche dati in formato digitale e in generale tutti i documenti prodotti tramite l'utilizzo dei suddetti apparati.

5. Il presente regolamento è destinato a tutti gli utenti, Interni ed Esterni, come di seguito definiti, che utilizzano un computer o un apparato telematicoricevuto in dotazione dalla Società e sono autorizzati ad accedere alla Rete Informatica e Telematica di Ade Spa, con sede operativain Parma, Viale Villetta 31/a.

6. Per utenti Interni s'intendono tutti i Dirigenti, i Responsabili di Servizio o Unità Operativa, gli Amministratori, i dipendenti a tempo indeterminato o determinato e i collaboratori occasionali.

7. Per utenti Esterni s'intendono: le ditte fornitrici di software che eseguono attività di manutenzione limitatamente alle applicazioni di loro competenza, Enti esterni autorizzati da apposite convenzioni all'accesso a specifiche banche dati con le modalità stabilite dalle stesse e collaboratori esterni a vario titolo.

ART. 2 - PRINCIPI GENERALI, DIRITTI, DOVERI E RESPONSABILITÀ

1. La Società promuove l'utilizzo della Rete Informatica e Telematica, di Internet e della Posta Elettronica quali strumenti utili a perseguire, con efficacia ed efficienza, le proprie finalità istituzionali, in accordo con le linee guida e i principi delineati dalla normativa vigente.

2. L'adozione di questo regolamento è fatta nell'intento di perseguire i seguenti scopi nella priorità elencata:

    a. garantire la massima sicurezza nell'accesso alla rete privata (intranet) e pubblica (internet);

    b. assicurare la massima efficienza nell'utilizzo delle risorse del Sistema Informativo;

    c. garantire la riservatezza delle informazioni e dei dati;

    d. garantire il rispetto delle leggi in materia di utilizzo delle risorse informatiche per l'elaborazione dei dati personali e sensibili (D.Lgs. 196/03 T.U. Privacy e regolamenti collegati);

e. informare con chiarezza i lavoratori sulle modalità di utilizzo di Internet e della posta elettronica e sulla possibilità che vengano effettuati controlli;

f. perseguire la massima flessibilità di servizio nell'interesse della produttività aziendale.

3. Ogni utente è responsabile, civilmente e penalmente, del corretto uso delle Risorse Informatiche, dei servizi/programmi cui ha accesso e dei dati trattati a fini istituzionali.

4. E' altresì responsabile del contenuto delle comunicazioni effettuate e ricevute a fini istituzionali anche per quanto attiene la riservatezza dei dati ivi contenuti, la cui diffusione impropria potrebbe configurare violazione del segreto d'ufficio o della normativa per la tutela dei dati personali.

5. Sono vietati comportamenti che possono creare un danno, anche d'immagine, alla Società.

6. Il presente regolamento è richiamato quale parte integrante nel contratto individuale di lavoro (o atto di instaurazione della collaborazione a vario titolo con la Società) ed è consegnato all'interessato, che lo sottoscrive per ricevuta.

7. La Società si riserva di compiere controlli sul corretto utilizzo degli strumenti informatici e telematici nel rispetto delle normative vigenti e del presente regolamento.

8. Per esigenze organizzative, produttive e di sicurezza la Società può avvalersi di strumenti che consentono un monitoraggio a distanza di tipo generalizzato, indiretto e anonimo, relativo all'intera struttura amministrativa, ad aree, settori o gruppi di utenti.

9. Qualora – durante un monitoraggio – siano rilevate anomalie nell'utilizzo degli strumenti informatici, la Società, tramite l'Amministratore di Sistema, procede preliminarmente all'invio di un avviso generalizzato relativo all'uso improprio riscontrato, con l'invito ad attenersi scrupolosamente al presente regolamento ed alle indicazioni impartite dal Direttore Generale, riservandosi la facoltà di svolgere successive azioni mirate alla puntuale verifica del corretto utilizzo.

10. Il mancato rispetto o la violazione delle norme contenute nel presente regolamento è perseguibile con provvedimenti disciplinari, nonché con le azioni civili e penali previste.

ART. 3 - ATTIVITÀ NON CONSENTITE NELL'USO DELLA RETE INFORMATICA E TELEMATICA

1. Nell'uso della Rete Informatica e degli apparecchi telematici non sono consentite le seguenti attività:

a. utilizzare la Rete in modo difforme da quanto previsto dal presente regolamento.

b. utilizzare la Rete per scopi incompatibili con le mansioni lavorative assegnate.

c. comunicare ad altri soggetti, interni o esterni all'azienda,o comunque rendere disponibili a terzi, i dati relativi al proprio account di rete (username e password). La password è segreta e strettamente personale.

d. agire deliberatamente con attività che influenzino negativamente la regolare operatività della Rete e ne restringano l'utilizzabilità e le prestazioni per altri utenti.

e. compiere trasferimenti, non autorizzati dal rispettivo Responsabile di Unità Operativa o di Servizio, dal Direttore Generale o dal Presidente C.d.A., di informazioni (software, dati, report o tabelle di attività; ecc.) o di documenti concernenti proprietà intellettuali di ADE SpA, o dell'Amministrazione Comunale;

f. salvare i dati della propria attività solo ed esclusivamente sul personal computer, evitando di utilizzare la partizione di server dedicato a ogni dipendente, sul quale sono eseguiti salvataggi periodici per motivi di sicurezza e custodia dei dati di proprietà della Società;

g. installare, eseguire o diffondere su qualunque computer e sulla rete aziendale, programmi destinati a danneggiare o sovraccaricare i sistemi o la rete (ad es. virus, cavalli di troia, worms, spamming della posta elettronica).

h. installare o eseguire software non autorizzati o non compatibili con l'attività lavorativa.

i. cancellare, copiare o asportare software per scopi personali, modificando così il profilo aziendale assegnato dall'Amministratore di sistema.

j. installare elementi hardware non compatibili con l'attività lavorativa o non espressamente richiesti e autorizzati dal Direttore Generale e dal Responsabile del Servizio Innovazione Tecnologica.

k. rimuovere, danneggiare o asportare elementi hardware, software o data base.

l. utilizzare qualunque sistema informatico o elettronico per controllare le attività di altri utenti, per leggere, copiare o cancellare files e software di altri utenti.

m. utilizzare software visualizzatori di pacchetti TCP/IP (sniffer), software di intercettazione di tastiera (keygrabber), software di decodifica password (cracker) e più in generale software rivolti alla violazione della sicurezza del sistema e della privacy;

n. inserire password locali alle risorse informatiche assegnate (come ad esempio password che non rendano accessibile il computer agli amministratori di rete), se non espressamente autorizzate dall'Amministratore del Sistema e obbligatoriamente comunicate all'Ufficio Sviluppo ed Innovazione Tecnologica;

o. la memorizzazione (su ogni tipo di supporto) e lo scambio di file relativi a materiale protetto da Copyright di cui ADE non abbia diritto d'uso (MP3, MP4, AVI, MPEG, DIVX, XVID, ecc.) nonché di materiale pornografico o lesivo della dignità ed eventuali altri tipi di file soggetti alla normativa sul diritto di autore e ad altre norme restrittive in materia di utilizzo del WEB.

p. modificare le configurazioni hardware e software predefinite dall'Amministratore di sistema e installare autonomamente programmi o applicativi senza preventiva autorizzazione.

q. la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per

sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

ART. 4 - AMMINISTRATORE DI SISTEMA – NOMINA E COMPITI

1. Il Direttore Generale nomina l'Amministratore di Sistema, sentito il Responsabile Informatico ed Innovazione Tecnologica tra i dipendenti che abbiano comprovata capacità professionale.

2. Nell'ambito dell'incarico l'Amministratore di Sistema, dovrà svolgere le seguenti funzioni:

   a. definire i requisiti di sicurezza da adottare per proteggere il complesso degli archivi di dati personali, delle procedure e dei sistemi informativi esistenti, osservando quanto prescritto dal d.lgs. 196/2003 e dal relativo disciplinare tecnico allegato sub B);

   b. realizzare ed implementare il sistema di sicurezza, in base ai requisiti di sicurezza definiti nel punto precedente, mediante l'adozione delle opportune misure tecniche e procedurali;

   c. gestire l'archivio e l'aggiornamento delle autorizzazioni, profili di accesso e collegamenti rilasciate direttamente o dal Direttore Generale;

   d. predisporre un piano di controlli periodici, da eseguirsi con cadenza almeno trimestrale, dell'efficacia delle misure di sicurezza adottate;

   e. predisporre e mantenere in efficienza i sistemi e le procedure di ripristino dei dati, nel caso in cui essi siano colpiti da eventi che possano danneggiarli o addirittura distruggerli, con l'obiettivo di renderli nuovamente disponibili entro un lasso di tempo ragionevole, avendo riguardo all'efficienza dell'organizzazione, ed in ogni caso non superiore ad una settimana per i dati di natura sensibile e per quelli giudiziari;

   f. effettuare la manutenzione del sistema di sicurezza, per assicurarne la costante efficienza e disponibilità, nonché procedere al suo aggiornamento periodico, per renderlo sempre adeguato alle nuove minacce;

   g. sottoporre alla Direzione Generale le richieste di risorse da destinare al miglioramento, mantenimento ed efficentamento della rete informatica, telematica e di comunicazione anche con piani previsionali poliennali.

All'Amministratore di Sistema, esclusivamente nei casi eccezionali previsti dal punto 10 dell'all.B (d.lgs. 196/03), è consentito l'accesso ai dati personali dell'utente (account di posta elettronica, files, ecc.). Ciò può avvenire solo in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabili e indifferibili interventi concernenti l'operatività e la sicurezza del sistema. In tali casi è comunque garantita la riservatezza dell'utente, il quale sarà tempestivamente informato dell'intervento effettuato e invitato a cambiare le proprie credenziali di autenticazione.

ART. 5 - **GESTIONE DELLE PASSWORD E DEGLI ACCOUNT**

1. L'account è costituito da un codice identificativo personale (username o user id) e da una parola "chiave" (password).

2. Si distinguono account di accesso al personal computer, di accesso alla rete e di accesso ai programmi autorizzati, ciascuno con una specifica password, in particolare:

   a) password di rete, per l'avvio e l'utilizzo del sistema operativo e di tutte le risorse di rete

   b) password per l'accesso a particolari programmi e applicativi.

3. Per incrementare il livello di sicurezza, la Società adotterà progressivamente l'utilizzo di sistemi di single sign on (autenticazione unica o identificazione unica) ovvero sistemi specializzati che consentono a un utente del sistema informatico di autenticarsi una sola volta e di accedere a tutte le risorse informatiche alle quali è abilitato.

4. Non è consentita l'attivazione della password d'accensione (bios), senza preventiva autorizzazione da parte dell'Amministratore di Sistema.

5. La password deve essere costituita da almeno otto caratteri che possono essere lettere (maiuscole e/o minuscole), numeri e caratteri speciali, evitando contenuti di senso logico immediato facilmente individuabile.

6. La password deve essere personale e segreta e deve essere tassativamente cambiata quando il sistema lo richiede (al massimo ogni tre mesi).

7. In caso di assenze prolungate e programmate, qualora se ne ravvisi la necessità, il dipendente potrà richiedere la sospensione dell'account. L'Amministratore di sistema avrà cura di assegnare una nuova password, per l'accesso temporaneo al PC, da parte di altro dipendente autorizzato. Al rientro il dipendente avrà cura, informando l'Amministratore di sistema, di sostituire nuovamente la propria password.

ART. 6 - UTILIZZO DEL PERSONAL COMPUTER, PC PORTATILE E HARD DISK RIMOVIBILI

1. I Personal Computer(PC) sono strumenti di lavoro: è vietato ogni utilizzo non inerente l'attività lavorativa. Non è consentito al dipendente di modificare le caratteristiche impostate sul proprio PC, salvo preventiva richiesta e successiva autorizzazione esplicita dell'Amministratore di sistema. L'utente è responsabile del PC assegnatogli e deve custodirlo con diligenza. Il PC deve essere spento ogni sera prima di lasciare gli uffici e ogni qual volta ci sia la necessità di allontanarsi dal posto di lavoro deve essere attivata la protezione tramite password (salvaschermo, lock computer), fatto salvo la/le postazioni utilizzate per i programmi di produzione che richiedono continuità operativa. Lasciare un elaboratore incustodito connesso alla rete, può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.

2. Ogni utente deve tenere comportamenti corretti, tali da preservare il buon funzionamento degli strumenti e tali da ridurre i rischi per la sicurezza del sistema informatico, quali l'utilizzo di supporti per la memorizzazione dei dati non sicuri e cd provenienti dall'esterno, al fine di non diffondere virus.

3. Tutti i PC forniti in dotazione sono protetti da apposito programma antivirus periodicamente aggiornato . Ai PC portatili si applicano le regole di utilizzo previste per i PC di cui sopra. Si

raccomanda una maggior attenzione per la criticità insita nello strumento informatico in oggetto.

4. I PC portatili impiegati all'esterno, quando non sono utilizzati, devono essere custoditi in un luogo protetto per prevenirne il furto.

5. Qualora sia indispensabile, per motivi legati a contratti di telelavoro, memorizzare sui PC portatili dati considerati sensibili dalla legge, richiedendo preventivamente ai responsabili aziendali e l'Amministratore di sistema l'autorizzazione, è obbligatorio l'utilizzo di tecniche di crittografia.

6. E' vietato l'utilizzo di hard disk rimovibili,per memorizzare documenti e dati provenienti dai programmi di proprietà della Società, senza preventiva autorizzazione del Direttore Generale e giustificato motivo.

ART. 7 - UTILIZZO DELLE STAMPANTI, FAX E DEI SUPPORTI DI MEMORIA MAGNETICI/OTTICI

1. Le stampe dimenticate o i dati memorizzati su supporti rimovibili possono spesso costituire involontaria fuga di notizie. Si raccomanda quindi la massima attenzione nell'utilizzo di stampe e dischetti o diversi dispositivi di memorizzazione con particolare riferimento alla corretta distruzione di documenti e o supporti che non sono più utilizzati. E' cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni. E' vietato portare fuori dall'azienda tabulati, stampe, supporti di memorizzazione sia magnetici che ottici salvo esplicita autorizzazione del Direttore Generale o del Presidente della Società. La stampa documenti può avvenire anche in modo riservato, previa digitazione di un codice identificativo dal PC dal quale si esegue la stampa e alla stampante all'atto del ritiro del documento da stampare.

2. Il servizio Fax è considerato, per motivi organizzativi, una parte del circuito di comunicazione aziendale e quindi è trattato con le stesse regole di un qualsiasi documento aziendale. Si invitano quindi gli utenti di non utilizzare il Fax aziendale per messaggi personali.

3. Tutti i supporti magnetici e/o ottici (chiavette USB, dischetti, cassette, CD-R, CD-RW, DVD-R, DVD-RD) contenenti dati sensibili devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato e cadere in mano a terzi non autorizzati. La semplice cancellazione dei supporti non garantisce l'eliminazione dei dati in essi memorizzati; una persona esperta potrebbe, infatti, recuperare i dati memorizzati anche dopo la loro cancellazione. Supporti magnetici o tabulati, contenenti dati sensibili devono essere custoditi in archivi chiusi a chiave come prescritto dalla Legge sulla tutela dei dati personali. In ogni caso non possono essere mai portati all'esterno, se non previa autorizzazione del Direttore Generale o del Presidente della Società.

ART. 8 - CONSERVAZIONE, CONSULTAZIONE E GESTIONE DEI DOCUMENTI CARTACEI

1. Tutti i documenti cartacei devono essere gestiti in modo da ridurre al minimo i tempi di permanenza al di fuori degli archivi o degli armadi o contenitori in dotazione alle unità operative. Massima attenzione dovrà essere posta per i documenti che si trovano in locali accessibili al pubblico.

2. L’accesso agli archivi è consentito al personale a ciò espressamente autorizzato in via permanente od occasionale. Gli archivi devono essere mantenuti, compatibilmente con le esigenze di servizio, costantemente chiusi. Le copie dei documenti vanno trattate, con riferimento alla tutela dei dati personali in esse contenuti, con la medesima diligenza riservata agli originali. Gli addetti ai servizi dove possono essere trattati dati sensibili o giudiziari dovranno porre massima attenzione al rispetto delle disposizioni precedenti. Essi inoltre dovranno limitare al minimo indispensabile la giacenza della documentazione al di fuori degli armadi o contenitori muniti di serratura; controllare con particolare rigore l’accesso ai propri archivi; autorizzare e registrare eventuali accessi negli uffici compiuti al di fuori degli usuali orari di chiusura.
3. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.
4. L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

ART. 9 - UTILIZZO DEGLI APPARECCHI E DISPOSITIVI TELEFONICI

1. Il telefono aziendale affidato all’utente è uno strumento di lavoro. La ricezione o l'effettuazione di telefonate personali è consentito esclusivamente secondo le disposizioni impartite dalla Società e che prevedono il recupero di costi a carico dell’utente, altrimenti mediante il telefono fisso aziendale a disposizione dell'utente. L’utente a cui è assegnato un cellulare aziendale è responsabile del suo utilizzo e della sua custodia. Al cellulare aziendale si applicano le medesime regole sopra previste per l’utilizzo del personal computer (vedi art. 5) e del telefono fisso aziendale.

ART. 10 - UTILIZZO DELLA POSTA ELETTRONICA E INTERNET

1. La casella di posta elettronica individuale è assegnata d’ufficio agli Amministratori, al Direttore Generale, ai Direttori o responsabili di Ufficio, di Coordinamento staff, ai dipendenti assunti a tempo indeterminato, determinato e ai collaboratori che, per le funzioni svolte, sono dotati di personal computer.

   Per particolari forme di lavoro, qualora le funzioni svolte richiedano l’uso della posta elettronica, la casella di posta elettronica individuale è assegnata su espressa richiesta del responsabile di riferimento.

2. La Società rende inoltre disponibili, oltre a quelli individuali, anche indirizzi di posta elettronica condivisi da più utenti. Tali indirizzi condivisi devono essere utilizzati esclusivamente per la ricezione di messaggi. Solo nel caso di particolari e specifiche necessità, (esempio caselle di posta elettronica certificata) e previa autorizzazione della struttura competente, le caselle di posta elettronica condivise potranno essere utilizzate per l’invio di messaggi o trasmissione di file. Il Dirigente o Responsabile di Servizio individua un responsabile di riferimento della gestione della casella di posta elettronica condivisa.

3. La casella di posta elettronica assegnata è uno strumento di lavoro e il suo utilizzo è consentito solo per finalità connesse allo svolgimento della propria attività lavorativa.Le persone assegnatarie sono responsabili del corretto utilizzo della stessa.

4. E' fatto divieto di utilizzare la casella di posta elettronica per:
   a) trasmettere dati sensibili, salvo i casi espressamente previsti dalla normativa vigente in materia di dati sensibili;
   b) trasmettere dati confidenziali e personali di alcun genere, salvo i casi espressamente previsti dalla normativa vigente in materia di protezione dei dati personali;
   c) partecipare a dibattiti, forum, o mail-list non attinenti la propria attività o funzione svolta per l'Ente, salvo diversa ed esplicita autorizzazione.

5. Non è consentito l'invio di messaggi con allegati di dimensione superiori a 3 Mb e con estensione uguali a .lnk .bat .exe .scr ed in generale file di tipo eseguibile o di applicazione. Si precisa che il sistema di sicurezza e antivirus installato a protezione del server di posta elettronica della Società non consente la ricezione e l'invio di messaggi di posta che contengono allegati con le caratteristiche sopra elencate. Eventuali esigenze particolari potranno essere segnalate alla struttura competente che individuerà la soluzione tecnica più appropriata.

6. In caso di assenze dal lavoro sia programmate che non programmate, l'interessato deve delegare un altro lavoratore a verificare il contenuto dei messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti ed urgenti per lo svolgimento dell'attività lavorativa.
7. In caso di cessazione del rapporto di lavoro, l'indirizzo di posta elettronica individuale dell'interessato è mantenuto attivo per un periodo pari a quattro settimane.

ART. 11 – CONTROLLI

1. La Società si riserva di effettuare controlli sull'uso degli strumenti elettronici nel rispetto dei principi normativi di " pertinenza e non eccedenza".

2. Il controllo di comportamenti anomali con verifiche preliminari su dati aggregati si conclude, nel caso di anomalia riscontrata, con avviso personale e riservato all'utente invitandolo ad attenersi scrupolosamente ai compiti assegnati e a quanto disposto con il presente regolamento.

3. E' attivo uno strumento di controllo della "navigazione" in internet che si fa carico di regolare l'accesso alla rete in sintonia con le esigenze di sicurezza del sistema informativo aziendale e di uso proprio delle dotazioni informatiche e telematiche.

ART. 12 - SANZIONI

1. Il mancato rispetto o la violazione delle norme contenute nel presente regolamento, segnalato all'utente, è perseguibile con provvedimenti disciplinari, previsti dal vigente CCNL, graduati secondo la gravità del caso e con le azioni civili e penali obbligatorie o previste dalla normativa vigente.

2. In caso di reiterate violazioni commesse dallo stesso soggetto o in casi di particolare gravità la Direzione Generale può proporre all'Azienda la inibizione permanente alle autorizzazioni di utilizzo della rete informatica aziendale con destinazione del soggetto responsabile a mansioni diverse e/o ridotte.

APPENDICE

GLOSSARIO DEI TERMINI TECNICI E INFORMATICI

Account	Iscrizione registrata su un server e che, tramite l'inserimento di una userld e di una password, consente l'accesso alla rete e/o ai servizi. Ad esempio, un account ci permette di entrare in Internet, un altro account ci serve per ricevere e spedire posta elettronica. Un account ci consente di accedere alle risorse di una rete locale, come server, file server, stampanti. Altri account servono per accedere a server e servizi vari.
Antivirus	Tipo di software che cerca e distrugge gli eventuali programmi virus e cerca di rimediare ai danni che hanno compiuto.
Backup	Copia di riserva di disco, di una parte del disco o di uno o più file.
Database	(Base di Dati). Qualsiasi aggregato di dati organizzato in campo (colonne) e record (righe).
Download	Registrare sul proprio disco rigido un file richiamandolo, tramite modem o rete, da un computer, da un server o da unhost (tramite Internet, rete locale o geografica).
E-mail	Electronic mail, posta elettronica. Scambio di messaggi e di file attraverso una rete locale o Internet. Avviene in tempo reale ed è indipendente dalla posizione fisica dei computer mittente e destinatario. I messaggi e file vengono conservati da un server che provvede ad inoltrarli al destinatario quando questo si collega.
Firewall	Insieme di software/hardware usato per filtrare i dati in scambio fra reti diverse, al fine di proteggere un server da attacchi pervenuti via rete locale o via Internet. Consente il passaggio solamente di determinati tipi di dati, da determinati terminali e determinati utenti.
Freeware	Software gratuito realizzato e distribuito da privati o piccole società, attraverso Internet o CD-ROM allegati a pubblicazioni in edicola.
Hardware	Letteralmente ferramenta, in informatica si intende l'insieme dei componenti (CPU, Hard Disk ecc.) che costituiscono un computer.
Internet	La madre di tutte le reti di computer. E' l'insieme mondiale delle reti di computer interconnesse.
Intranet	Rete locale che, pur non essendo necessariamente accessibile dall'esterno, fa uso di tecnologie Internet.

MP3 (MPEG-4)	Tecnologia per la compressione/decompressione di file audio che consente di mantenere una perfetta fedeltà e qualità anche riducendo il file audio di ben 11 volte la lunghezza originale.
MPG (Motion Picture Experts Group)	Stabilisce gli standard digitali per audio e video.
Password	Parola che consente l'accesso di un utente ad una rete, ad un servizio telematico o ad un sito Internet. E' necessario digitarla esattamente, assieme alla user-id.
Quicktime	Standard definito dalla Apple e utilizzato da tutti i computer per la riproduzione fedele dei filmati video.
Software	Sono i programmi (professionali, ludici, video, musicali, raccolte di suoi ed immagini) per i computer.
Streaming	Con il termine **streaming** si intende un flusso di dati audio/video trasmessi da una sorgente a una o più destinazioni su Internet.
Url filtering	Sistema che permette di monitorare e filtrare la navigazione in Internet, bloccando l'accesso a particolari categorie di siti, al fine di limitare il rischio di utilizzo improprio della rete e la navigazione in siti non pertinenti o non compatibili con l'attività aziendale.
User Id	Nome utente
Utente (User)	Chiunque utilizzi un elaboratore collegato alla rete, sia che il collegamento avvenga in rete locale sia che si tratti di un accesso remoto.
Virus	Un programma creato per diffondersi da computer a computer, spesso danneggiando i dati e gli altri programmi registrati.