Regolamento di utilizzo dei sistemi informatici.

INDICE:

1: Scopo ed ambito di applicazione

Scopo della presente procedure è di disciplinare e divulgare le condizioni ed i limiti entro cui gli utenti possono legittimamente usare le informazioni aziendali, le postazioni di lavoro, i servizi Internet/Intranet ed ogni altro strumento o dispositivo informatico e telematico messo a disposizione dall'azienda, evitando di esporre se stessi e/o le Società in ambito di applicazione a sanzioni pecuniarie e/o penali o in generale ridurre il livello di sicurezza dell'organizzazione.
Il presente regolamento viene emesso anche in attuazione delle prescrizioni dei modelli ex
D.Lgs. 231/01 adottati dalle società in ambito di applicazione al fine di prevenire, fra l'altro, la commissione dei c.d. reati informatici ed in conformità al Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali".
Il regolamento deve essere recepito ed applicato dagli utenti che utilizzano, a qualsiasi titolo, le risorse informatiche aziendali.
Per risorse si intendono:

- *Postazioni di lavoro*
- *Servizi di rete(posta, directory aziendale, portali interni, server, internet, etc…).*

L'accesso alla postazione di lavoro, informazioni, sistemi/servizi, da parte degli utenti, non potrà avvenire senza aver preventivamente recepito le prescrizioni e le indicazioni ivi contenute.
Gli utenti sono consapevoli che il mancato rispetto di quanto prescritto è passibile di sanzioni disciplinari e/o penali e se ne assumono la responsabilità, come da codice disciplinare o da CCNL.

2: Riferimenti normativi

Art. 2049 C.C e **Art. 40 C.P.:** *Il datore di lavoro è responsabile delle azioni del dipendente:"reati omissivi".*

Codice Penale:
Art. 600-quater: *Detenzione di materiale pornografico. Chiunque, al di fuori delle ipotesi previste dall'articolo 600-ter, consapevolmente si procura o detiene materiale pornografico realizzato utilizzando minori degli anni diciotto, è punito con la reclusione fino a tre anni e con la multa non inferiore a euro 1.549. La pena è aumentata in misura non eccedente i due terzi ove il materiale detenuto sia di ingente quantità.*
Art. 600-quater bis: *Pornografia virtuale. Le disposizioni di cui agli articoli 600-ter e 600-quater si applicano anche quando il materiale pornografico rappresenta immagini virtuali realizzate utilizzando immagini di minori degli anni diciotto o parti di esse, ma la pena è diminuita di un terzo. Per immagini virtuali si intendono immagini realizzate con tecniche di elaborazione grafica non associate in tutto o in parte a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali.*
Art. 615-ter: *Accesso abusivo ad un sistema informatico o telematico.*
Art. 615-quater: *Detenzione e diffusione abusiva di codici i accesso ai sistemi informatici o telematici.*
Art. 615-quinquies: *Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informativo o telematico.*
Art. 617-quater: *Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche.*
Art. 617-quinquies: *Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche.*

Art. 635-bis: *Danneggiamento di informazioni, dati e programmi informatici.*
Art. 635-ter: *Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità.*
Art. 635-quater: *Danneggiamento di sistemi informatici o telematici.*
Art. 635-quinquies: *Danneggiamento di sistemi informatici o telematici di pubblica utilità.*
Art. 640-quinquies: *Frode informatica del soggetto che presta servizi di certificazione di firma elettronica.*
Art. 491-bis: *Falsità di documenti informatici.*
Decreto Legge 22 marzo 2004 n.72 *convertito in legge con modificazioni dalla legge 21 Maggio 2004 n. 128 (Legge Urbani) che sanziona la condivisione e/o fruizione di file relativi ad un'opera cinematografica od assimilata protetta da Diritti d'autore.*
D.Lgs 196/2003 – *Codice in materia di Protezione dei Dati Personali (Testo Unico).*
Legge n.*547/1993* *Legge sui crimini informatici.*
Legge 48/2008 *relativa al Cyber Crime.*
Legge n.633/1941 *e successive modificazioni (tutela del diritto d'autore).*
D.Lgs 231/01
Legge 300/1970 *tutela della libertà e dignità dei lavoratori.*
Policy Enterprice Risk Management
Si rimanda al modello di organizzazione gestione controllo aziendale ai sensi D.Lgs.231/01 parte speciale A (pag.11) e parte speciale D (Pag. 13-14-15)

3: Definizioni

RISORSE: *strumenti e informazioni che costituiscono il patrimonio tangibile e intangibile dell'azienda.*
INFORMAZIONI:
*"**dato personale**", qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;*

*"**dati sensibili**",i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche , l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico , politico o sindacale nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;*
Informazioni riservate: *E' considerata informazione riservata qualunque notizia di carattere confidenziale inerente la Società o il Gruppo, di cui si venga a conoscenza in ragione della propria funzione. E', a titolo esemplificativo, da considerarsi riservata la conoscenza di un progetto, una proposta, un'iniziativa, una trattativa, un'intesa, un impegno, un accordo, un fatto o un atto, anche se futuro o incerto, attinente la sfera di attività di COSMO S.p.A. e delle società da esse controllate, che non sia di dominio pubblico.*
Informazioni privilegiate: *Le informazioni privilegiate costituiscono un sottoinsieme delle informazioni riservate. Ai sensi dell'art. 181, comma 1 del TUF, per informazione privilegiata si intende "ogni informazione del carattere preciso, che non sia stata resa pubblica, concernente, direttamente o indirettamente, uno o più emittenti strumenti finanziari o uno o più strumenti finanziari che, se resa pubblica, potrebbe influire in modo sensibile sui prezzi di tali strumenti finanziari".*

UTENTI: *si intende tutto il personale (interno ed esterno), autorizzato ad utilizzare, anche in via temporanea, le attrezzature e i sistemi della Società in ambito di applicazione.*
RESPONSABILE DELLA SICUREZZA DELLE INFORMAZIONI*: si intende uno o più responsabili del Gruppo a cui l'Alta Direzione affidi l'incarico di monitorare lo stato di implementazione e di efficienza delle misure di protezione adottate oda adottare al fine di garantire la riservatezza, l'integrità e la disponibilità delle risorse informatiche aziendali.*
RESPONSABILE DEL DATO: *si intende responsabile di funzione incaricato di definire i profili di accesso ai dati di business che tratta, nonché valutare le richieste di fruizione dei medesimi dati.*

4: Responsabilità

La responsabilità per l'esecuzione è di tutto il personale che svolge le attività descritte in tale documento.
L'utente autorizzato ad accedere alle risorse delle Società in ambito di applicazione, deve essere consapevole delle conseguenze derivanti da azioni e componenti illeciti o non conformi al presente regolamento.
L'utente si impegna a rispettare le procedure e le politiche di sicurezza fornite dall'organizzazione, contribuendo al mantenimento della sicurezza delle informazioni.

5: Descrizione

Tutte le informazioni/dati devono essere usate esclusivamente per gli scopi aziendali espressamente autorizzati. Ove non strettamente necessario (e comunque previa approvazione del responsabile di funzione) si fa divieto di condividere informazioni con esterni, o con personale non autorizzato. E' fatta esplicita richiesta di far valere il principio del buon senso e di riservatezza, limitando a quanto strettamente necessaria la divulgazione delle stesse.

L'utilizzo degli strumenti e delle risorse informative aziendali deve essere strettamente vincolato all'esercizio delle attività lavorative, rispettando le normative aziendali e in ottemperanza alle disposizioni legislative vigenti. E' proibito l'impiego delle risorse aziendali per scopi personali o di terzi; in particolare si fa divieto esplicito di:

- *Utilizzare le risorse aziendali per profitto personale*
- *Impiegare le risorse per finalità diverse da quelle per le quali sono state progettate o utilizzare i sistemi informativi per compiere azioni illecite nei confronti di altri sistemi, sia interni che esterni all'organizzazione;*
- *Recare, volontariamente danni alle risorse aziendali, agli strumenti di supporto, ai locali ed in generale ai dispositivi informatici utilizzati dall'organizzazione.*

Ogni strumento o risorsa, concessa ai fini esclusivamente lavorativi, deve essere correttamente custodita e mantenuta in buono stato dall'utente che deve contribuire, in rapporto alle proprie responsabilità, alla protezione dell'intero patrimonio delle Società in ambito di applicazione.

5.1 Postazioni di lavoro

La Postazione di Lavoro (di seguito postazione) è costituita dall'insieme di componenti hardware e software forniti all'utente dall'azienda. Essa consente l'accesso al complesso dei sistemi e servizi resi disponibili.

L'utente è consapevole e accetta di restituire la totalità delle risorse utilizzate nel momento in cui cessa il rapporto con la Società in ambito di applicazione.
Ogni utente, di norma, è assegnatario o autorizzato all'uso di una sola postazione, fissa o mobile; è responsabile delle medesima e deve custodirla con diligenza (sia all'interno dell'edificio aziendale, sia al di fuori), nonché segnalare eventuali furti, danneggiamenti o smarrimenti.
Inoltre è tenuto a prestare la massima collaborazione sia alle attività di censimento ed inventario delle risorse hardware e software, sia alle attività di aggiornamento di tali risorse.
Di seguito sono riportate le istruzioni operative per il corretto e sicuro utilizzo delle risorse hardware e software che costituiscono la postazione e dei sistemi e servizi informatici a cui l'utente può accedere attraverso la stessa.

5.1.1 Credenziali di accesso

1. *L'accesso al Sistema Informativo Aziendale delle Società in ambito di applicazione prevede l'utilizzo di un identificativo univoco (User-ID) e di una password necessari a dimostrare la propria identità al sistema o all'applicazione a cui si sta effettuando l'accesso. Per alcuni casi specifici possono essere adottati sistemi di identificazione ed autenticazione alternativi, come ad esempio l'utilizzo di lettori di impronte digitali, smart card, certificati digitali ecc, che forniscono livelli di sicurezza più elevati, conformemente a quanto previsto; tali dispostivi sono strettamente personali e non devono essere ceduti o comunicati a terzi.*
2. *Le regole implementate relative alle credenziali di accesso (utente e password) sono contenute in specifici documenti operativi redatti dalle singole società del Gruppo.*
3. *La postazione e gli eventuali supporti di memoria rimovibili (floppy disk, compact disk, chiavi USB, ecc.) devono essere conservati in luoghi protetti (ad esempio, armadi e cassettiere chiusi a chiave). E' sempre necessario verificare il contenuto informativo dei supporti di memoria, prima della loro consegna a terzi e prima della loro eliminazione/distruzione.*
4. *L'utente non è autorizzato ad accedere, né a tentare l'accesso alle informazioni per le quali non ha alcun privilegio; è altresì vietato tentare di guadagnare privilegi non concessi dal proprietario del dato.*

5.1.2 Hardware e software

1. *Non è permesso sottrarre dispositivi, apparecchiature e/o informazioni, in esse contenute, di proprietà dell'azienda.*
2. *L'utente non deve modificare la configurazione hardware e software della postazione di lavoro (fissa e/o mobile), aggiungendo o rimovendo componenti, rispetto allo standard definito e fornito dall'azienda, al fine di non danneggiare e/o interrompere il sistema informativo o telematico dell'azienda (C.P. – art.615 quinquies, art 615 quinquies). Qualora necessario l'utente può richiedere, previa verifica da parte del proprio responsabile, l'aggiornamento della propria configurazione hardware rivolgendosi alle funzioni competenti.*
3. *Non è consentito l'uso di programmi non distribuiti e/o installati ufficialmente dalla Direzione Sistemi Informativi.*

- ✓ *Non è consentito fare il download, da Internet o provenienti da soggetti esterni all'organizzazione e di installare il software non autorizzato (anche se freeware) sulla propria postazione, onde evitare il grave pericolo di introdurre virus informatici, nonché di alterare la stabilità delle applicazioni dell'elaboratore (C.P. –art. 615 quinquies, art 617 quinquies).*
- ✓ *Il software acquistato dal Gruppo è soggetto a limitazione nell'utilizzo e, a meno di una specifica autorizzazione concessa dallo sviluppatore dello stesso, nessun utente ha il diritto di riprodurlo, salvo che per motivi di salvataggio (opportunamente documentati). Inoltre non è consentito adattare, trasformare, distribuire software in licenza d'uso aziendale, in conformità alla legge sul Copyright; in considerazione degli obblighi imposti dal d.lgs.29 dicembre 1992, n.518, sulla tutela giuridica del software, e dalla l. 18 agosto 2000, n. 248, contenente nuove norme di tutela del diritto d'autore.*
- ✓ *La manutenzione software deve essere fatta solo dal personale autorizzato e competente. Pertanto si raccomanda a ciascun utente di rivolgersi sempre alla struttura preposta.*
- ✓ *Sui PC dotati di scheda audio e/o di lettore CD non è consentito l'ascolto di programmi e files audio o musicali, se non a fini prettamente lavorativi.*

In caso di necessità di software, rivolgersi, per qualsiasi richiesta, solo alla struttura di help desk di riferimento che valuterà il rilascio del software richiesto in conformità alle regole aziendali in vigore e, se necessario, sottoporrà la richiesta all'attenzione della Direzioni componenti.

4. *E' assolutamente vietato installare modem, schede di rete, schede Adsl, schede wireless o qualsiasi altro dispositivo di connessione senza autorizzazione del proprio responsabile e della Direzione Sistemi informativi. Qualora la postazione di lavoro sia dotata di una scheda modem è severamente vietato il suo impiego all'interno del perimetro dell'azienda, poiché costituirebbe un punto di accesso diretto alla intranet aziendale; in caso di assoluta necessità, solo previa autorizzazione delle strutture competenti e per un tempo limitato, l'accesso con questa modalità deve avvenire disattivando ogni altro dispositivo di connessione alla rete aziendale.*
   Non è consentito l'accesso alle infrastrutture centralizzate, sia in senso fisico sia attraverso collegamento remoto, senza preventiva autorizzazione della Direzione Sistemi Informativi se non con i profili stabiliti in base alle esigenze dell'utilizzatore e nel rispetto della normativa vigente in materia di sicurezza e privacy e dei reati cosiddetti informatici.

5. *L'Organizzazione interpreta in maniera estensiva i contenuti del codice penale in materia di Detenzione di materiale pornografico e di pornografia virtuale (art. 600-quater e 600-quater bis): E' FATTO ESPRESSO DIVIETO DI DETENERE, ALL'INTERNO DELLE STRUTTURE DEL GRUPPO E NELLE RELATIVE RISORSE INFORMATICHE, MATERIALE PORNOGRAFICO IN QUALSIASI FORMA E SU QUALUNQUE SUPPORTO, A PRESCINDERE DAI CONTENUTI E DALL'ETA' DELLE PERSONE COINVOLTE PER LA SUA REALIZZAZIONE.*

La disponibilità di informazioni complete circa la configurazione e la consistenza delle postazioni consente di monitorare costantemente la presenza di situazioni di rischio e di individuare gli aggiornamenti di sicurezza che consentono di ridurre tali rischi.

6. *E' assolutamente vietato utilizzare e/o installare software atti ad intercettare, falsificare, alterare il contenuto di documenti informatici, ad esempio programmi di recovery password, cracking, sniffing, spoofing, serial codes, ecc. (C.P. – art 615 quinquies)*
7. *Qualora per motivi di lavoro si sia in possesso di autorizzazioni atte ad accedere a sistemi informativi di Pubblica Utilità e/o dello Stato e/o di Ente Pubblico è fatto espresso divieto di mettere in atto comportamenti atti al danneggiamento di informazioni, dati e/o programmi dei suddetti soggetti (C.P. – art 635 ter, quater).*

Nel caso in cui l'utente venga a conoscenza di una qualsiasi vulnerabilità derivante da difetti di configurazione o difetti intrinseci ai programmi e/o ai sistemi non deve assolutamente sfruttarla per commettere azioni illecite o non autorizzate, bensì deve tempestivamente informare la funzione Sistemi Informatici.

5.1.3 Antivirus

1. *Ogni postazione è dotata del software antivirus standard aziendale, correttamente configurato ed aggiornato; è vietato disabilitare o inibire il corretto funzionamento del software antivirus. L'utente deve accertarsi che, sulla propria postazione di lavoro, il software antivirus aziendale sia sempre aggiornato e funzionante, secondo le modalità stabilite dalle apposite procedure. E' vietato disattivare il software antivirus o modificarne la configurazione, né disabilitare o disattivare i meccanismi di notifica automatica degli eventi e di segnalazioni degli allarmi.*
2. *Qualora per la propria postazione di lavoro non esista un software antivirus rispondente alle norme, o non sia possibile installare correttamente il software antivirus Aziendale, l'utente dovrà informare immediatamente il suo responsabile.*
3. *Nel caso che il software antivirus rilevi la presenza di un virus che non è riuscito ad eliminare, l'utente deve immediatamente sospendere ogni elaborazione in corso, senza spegnere il computer e segnalare l'accaduto alle funzioni competenti.*
   Gli utenti non possono rimuovere virus con azioni personali, ma devono avvalersi dell'assistenza necessaria, attenendosi alle modalità operative per la gestione degli incidenti; ad operazione ultimata, devono accertarsi dell'eliminazione del virus e della riusabilità della postazione di lavoro.

La direzione Sistemi Informatici provvede a scansire con il programma antivirus gli allegati che vengono ricevuti attraverso la casella di posta elettronica al fine di prevenire danni alle informazioni residenti in azienda.

5.1.4 Protezione dei dati

1. Crittografia: *E' proibito cifrare le informazioni, nonché trasmettere, salvare o ricevere informazioni cifrate, salvo in casi in cui si ottenga preventiva autorizzazione dal proprio responsabile, o non vi siano disposizioni operative che ne regolamentano l'impiego in casi particolari (es. trasmissioni ai fini lavorativi di informazioni sensibili).*
   nel caso di autorizzazione alla cifratura una chiave di crittografia deve essere conservata in maniera opportuna ad esempio su smart cards, tokens, etc.
2. Clear desk e screen policy
   - ✓ *Durante l'espletamento della propria attività lavorativa, l'utente deve prestare attenzione a non divulgare accidentalmente informazioni aziendali a personale non*

autorizzato, eventualmente presente nelle immediate vicinanze. Nel caso di assenza prolungata, e comunque al termine della normale attività lavorativa giornaliera, l'utente deve rimuovere dalla propria area di lavoro le informazioni ed i documenti, di cui dispone, riponendole in luoghi idonei (armadi o cassettiere con serratura, casseforti, etc). I documenti che contengono informazioni riservate non devono essere, in nessun caso, lasciati incustoditi sulle scrivanie.

- ✓ *In caso di assenza momentanea della propria postazione, l'utente deve bloccarla utilizzando la password dello screen saver (funzionalità del sistema operativo di Windows); a fine giornata lavorativa la Postazione di Lavoro deve essere spenta seguendo la procedura di Logoff.*

3. Utilizzo dei sistemi di riproduzione
   - ✓ *Durante la stampa, fotocopie o trasmissione fax di informazioni non pubbliche, da/a postazioni remote, l'utente deve presidiare ed assistere all'intero processo, in modo da impedire la volontaria o accidentale perdita di riservatezza sulle informazioni cartacee stampate. A tal riguardo è dovere dell'utente prelevare immediatamente i foglio riprodotti da stampanti, fotocopiatrici e fax.*

5.2 Servizi di rete

Le credenziali che consentono l'accesso all'internet aziendale e ai relativi servizi (portali interni, repositori documentali, posta elettronica, applicazioni, etc.) sono personali ed individuali, conseguentemente non possono essere condivise o cedute a terzi. L'utilizzo delle informazioni delle documentazione acquisita tramite l'internet aziendale è classificata d "uso interno", pertanto l'utilizzo è limitato alla sola attività lavorativa e sempre nel rispetto della legge sul copyright. L'utente deve tenere un comportamento politicamente corretto nell'utilizzo della rete aziendale, al tal riguardo, non deve effettuare nessun tipo di attività volta ad eludere o compromettere i meccanismi di protezione dei sistemi informatici.

5.2.2 Rete aziendale

L'integrità e la disponibilità dei dati aziendali è garantita dall'organizzazione solo quando questi sono memorizzati e trattati su memorie di massa o aree dedicate (ad esempio "personal network folder"), assegnate a ciascun utente. L'utente è tenuto a :

- ✓ *Trasferire la propria cartella dati, eventualmente presenti localmente sul proprio pc, considerati critici per l'azienda.*
- ✓ *Non condividere in rete i file, cartelle, programmi, senza preventiva autorizzazione dal proprio responsabile e dalla direzione sistemi informativi.*
- ✓ *Non distruggere o eliminare informazioni sensibili per l'azienda, senza preventiva autorizzazione.*

L'azienda si riserva la facoltà di procedere alla rimozione di goni file o applicazione che riterrà essere pericolosa per la sicurezza del sistema ovvero acquisiti o installati in violazione del presente violamento.

5.2.2 Internet

- *Internet è uno strumento messo a disposizione agli utenti dalla direzione aziendale. Affinché sia garantita la tutela dell'ambiente e dell'organizzazione che accede al servizio è necessario rispettare le seguenti regole:*
- *Non è consentita la navigazione, la registrazione e la memorizzazione di documenti informatici di natura contagiosa, pornografica e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.*
- *Non è consentito scaricare software gratuiti (freeware e shareware) prelevati da siti internet se non espressamente autorizzato dalle strutture competenti, e in ogni caso tutti i file di provenienza incerta o esterna, ancorché attinenti all'attività lavorativa, devono essere sottoposti al controllo antivirus. E', altresì, proibito scaricare video, brani musicali, giochi e materiali coperto da diritto d'autore.*
- *Non è consentito lo scambio (ad esempio Peer-to-Peer) a qualsiasi titolo, anche se non a scopo di lucro, di materiali audiovisivo, cinematografico, fotografico, informatico, etc, protetto da copyright.*
- *Non è consentito effettuare ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti online e simili, salvo casi direttamente autorizzati dal proprio responsabile e con il rispetto delle normali procedure di acquisto.*
- *Non sono permesse, per motivi non professionali, la partecipazione a forum, utilizzo di chat line o di bacheche elettroniche, anche utilizzando pseudo mini.*
- *Per non compromettere la funzionalità delle rete aziendale eventuali necessità di scarico dati e/o memorizzazione di file di grandi dimensioni devono essere autorizzate dalla struttura sistemi informativi.*
- *Non è consentito connettere gli strumenti informatici aziendali (personal computer, palmari, etc) a reti esterne pubbliche (internet) o private (sistemi di altre società) per mezzo di collegamenti fisici con linee telefoniche dedicate (ad esempio PSTN, ISDN, xDSL), reti mobili cellulari o con strumenti wireless di qualsiasi genere senza un'esplicita autorizzazione.*
- *Prima di autorizzare un fonte, un'informazione, testi o immagini, all'interno di propri lavori, è opportuno richiedere l'autorizzazione della fonte, citandola esplicitamente nel proprio documento (come previsto dalla legge sul copyright – diritto d'autore).*

5.2.3 Posta elettronica

La posta elettronica aziendale è uno strumento messo a disposizione agli utenti dalla direzione aziendale. Per una corretta fruizione del servizio di posta elettronica che tuteli l'utente e l'organizzazione devono essere rispettate le seguenti regole:

- *Ogni comunicazione (interne o esterna), inviata o ricevuta, che abbia contenuti rilevanti o contenga impegni per una o più società in ambito di applicazione deve essere visionata o autorizzata dal responsabile dell'unità organizzativa di appartenenza.*
- *Non è consentito inviare o memorizzare messaggi di natura oltraggiosa, volgare e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica. E' altresì vietato partecipare a "catene di Sant'Antonio" poiché si configurano come atti di "spamming" e la diffusione incontrollata di tali messaggi potrebbe impattare sull'efficienza del sistema di posta.*
- *Non è consentito l'utilizzo di posta elettronica aziendale per la partecipazione a dibattiti, forum, o mailing-list, salvo diversa ed esplicita autorizzazione. L'iscrizione ad una mailing-list o a servizi simili (chat, forum, etc) è consentita solo se funzionale all'attività aziendale.*
- *Ogni comunicazione massiva ovvero estesa a tutti i dipendenti di società tra quelle in ambito di applicazione, anche creando sottogruppi attraverso la scomposizione dei destinatari – dovrà essere preventivamente autorizzata dal proprio responsabile o dalla direzione dei sistemi operativi.*

- *La posta elettronica non deve essere utilizzata per ricevere, memorizzare o spedire materiale che violi il copyright, il marchio o altre leggi sul diritto d'autore (cfr. leggi sul diritto d'autore d.lgs. 68-83.*
- *L'utente deve ricordare che ogni comunicazione effettuata attraverso posta elettronica può essere intercettata, letta, copiata, modificata e inviata ad un altro indirizzo di conseguenza, nessun informazione strategica dovrebbe essere trasmessa attraverso questo sistema, a meno che venga trasmessa attraverso una forma cifrata autorizzata.*
- *E' opportuno assicurarsi che il destinatario dell'E-mail sia effettivamente quello desiderato. Nel caso in cui si commetta un errore nella spedizione di una mail occorre contattare il destinatario, chiedendogli di cancellare il messaggio.*
- *Nel caso di emittenti sconosciuto o messaggi insoliti, per non correre il rischio di essere infettati da codici maligni, occorrerà cancellare i messaggi senza aprirli. In ogni caso è obbligatorio controllare tutti i file in allegato prima del loro utilizzo e non eseguire il download di file eseguibili. In caso di dubbi, contattare immediatamente la direzione di sistemi informativi.*

5.2.4 Telelavoro

L'utente può usufruire dei privilegi che l'organizzazione garantisce relativamente all'impiego del telelavoro. Egli deve tuttavia rammentare che i privilegi potrebbero essere rivalutati, e addirittura sospesi, qualora l'organizzazione abbia riscontro di ritenere che la gestione della postazione di lavoro non sia in grado di assicurare un'adeguata protezione dei requisiti di riservatezza, disponibilità e integrità delle informazioni dell'organizzazione. Gli utenti che occupano postazioni di lavoro remote, operando per mezzo del telelavoro, devono aderire, come accade per utenti che operano in sede, a tutto ciò che viene imposto dall'organizzazione relativamente all'utilizzazione e trattamento degli strumenti e delle informazioni aziendali a cui sono in possesso. gli utenti che si adoperano attraverso il telelavoro, devono prontamente riferire all'organizzazione ogni trasferimento o cambiamento di residenza.

5.3 Controllo e monitoraggio delle risorse

Poiché in caso di violazioni giuridiche sia le società in ambito di applicazione sia il singolo lavoratore sono potenzialmente perseguibili con sanzioni, l'azienda periodicamente procederà nel rispetto delle garanzie di tutela dei dati personali previste dal testo unico d.lgs. 196-2003 ad un controllo quantitativo dell'utilizzo della rete, dei pc e della posta elettronica per verificarne un uso equilibrato e conforme all'attività e alle politiche aziendali.
In particolare, controlli periodici possono essere effettuati su :

- *Il volume dei messaggi scambiati*
- *Il formato dei file allegati*
- *La durata dei collegamenti ad internet (globale, per funzione)*
- *I siti più visitati più frequentemente (globale, per funzione)*
- *Le informazioni raccolte dai dispositivi di sicurezza (firewall, antivirus, IDS, etc.) per rilevare e contrastare situazione di illecito, ai sensi della l. 547-93 in materia di criminalità informatica.*

Il monitoraggio non è finalizzato al controllo delle attività degli utenti (salvo eventuale esplicita richiesta intersenso da parte delle autorità competenti). Le informazioni raccolte consento un controllo dell'efficienza e dell'utilizzo corretto delle risorse informatiche aziendali e del network. I dati sopra descritti sono acquisiti informa anonima e quindi non riconducibili alle identità del singolo utente. I dati sono archiviati, con le misure di sicurezza opportune, nei limiti sanciti dal decreto sulla privacy (D.lgs. 196-03) e le norme antiterrorismo (D.lgs. 144-05), fatto salvo di eventuali esplicite richieste della autorità competenti.

5.4 Osservanza del regolamento

La non osservanza del presente ordinamento può comportare sanzioni disciplinari, civile, penali. I dipendenti dell'azienda che vengono a conoscenza di qualunque uso improprio del software o della relativa documentazione devono informare la direzione sistemi informativi. La direzione sistemi informativi dovrà segnalare alla direzione del personale tutti i casi di non osservanza del regolamento rilevati nell'esercizio della propria attività e all'organismo di vigilanza i comportamenti che potrebbero configurare il rischio di commissione di un reato ex. D.lgs. 231-01.

5.4.1. Uso personale delle risorse aziendali

Internet, come la posta elettronica sono servizi che la società in ambito di applicazione forniscono i propri utenti per scopi aziendali. L'uso, esclusiva mento occasionale, di internet e della posta elettronica per scopo personale sarà tollerato solo se questo non avrà un effetto negativo sul livello della performance dei sistemi o sull'attività lavorativa generale. In ogni caso l'utente dovrà tener conto che la posta elettronica e l'utilizzo di internet potranno essere oggetto di attività di monitoraggio e/o di salvataggio (backup). A tal fine sono presenti filtri preventivi per impedire l'accesso a siti non autorizzati (web filtering) e scambio di E-mail con domini ritenuti non sicuri (anti-spam).