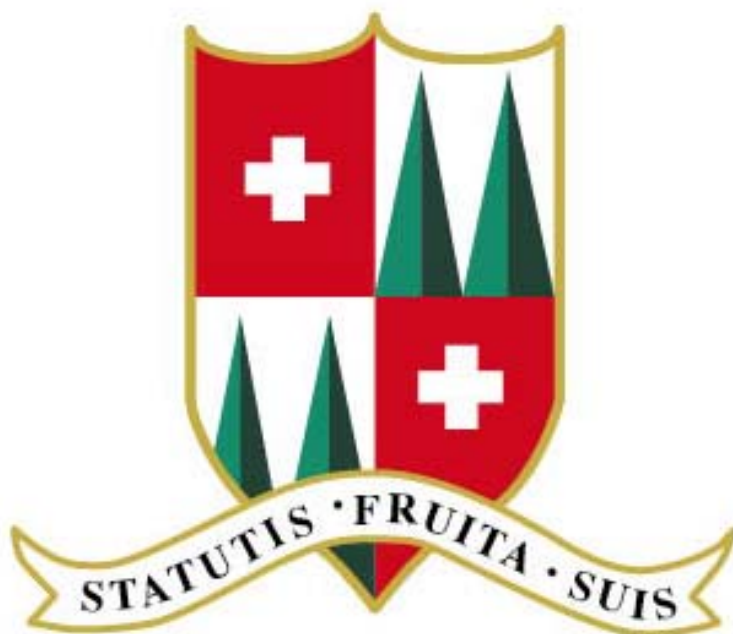


COMUNE DI SAN PELLEGRINO TERME



REGOLAMENTO PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI E TELEMATICI

Approvato con delibera n. 13 Consiglio Comunale del 17/08/2011

Regolamento Comunale per il Corretto Utilizzo degli Strumenti Informatici e Telematici

Le realtà aziendali si caratterizzano per l'elevato uso della tecnologia informatica che da un lato ha consentito l'introduzione di innovative tecniche di gestione dell'impresa, dall'altro ha dato origine a numerose problematiche relative all'utilizzo degli strumenti informatici forniti dall'azienda al dipendente per lo svolgimento delle proprie mansioni.

In questo senso, viene fortemente sentita dai datori di lavoro la necessità di porre in essere adeguati sistemi di controllo sull'utilizzo di tali strumenti da parte dei dipendenti e di sanzionare conseguentemente quegli usi scorretti che, oltre ad esporre l'azienda stessa a rischi tanto patrimoniali quanto penali, possono di per sé considerarsi contrari ai doveri di diligenza e fedeltà previsti dagli artt. 2104 e 2105 del codice civile e dall'art. 23 del CCNL. I controlli preventivi e continui sull'uso degli strumenti informatici devono garantire tanto il diritto del datore di lavoro di proteggere la propria organizzazione, essendo i computer aziendali strumenti di lavoro la cui utilizzazione personale è preclusa; quanto il diritto del lavoratore a non vedere invasa la propria sfera personale, e quindi il diritto alla riservatezza ed alla dignità come sanciti dallo Statuto dei lavoratori e dal D.lgs 196/03 sulla tutela dei dati personali.

Il Regolamento Comunale di seguito riportato viene incontro a tali esigenze disciplinando le condizioni per il corretto utilizzo degli strumenti informatici da parte dei dipendenti, in particolare alla luce degli obblighi previsti dal D.lgs 196/03 relativi all'adozione delle misure minime di sicurezza per il trattamento dei dati personali.

INDICE

Premessa

- 1) Utilizzo del Personal Computer
- 2) Utilizzo della rete
- 3) Gestione delle Password
- 4) Utilizzo dei supporti magnetici
- 5) Utilizzo di PC portatili
- 6) Uso della posta elettronica
- 7) Uso della rete Internet e dei relativi servizi
- 8) Protezione antivirus
- 9) Osservanza delle disposizioni in materia di Privacy
- 10) Controlli e responsabilità
- 11) Aggiornamento e revisione

PREMESSA

La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete Internet dai Personal Computer, espone il **Comune di San Pellegrino Terme** ai rischi di un coinvolgimento sia patrimoniale sia penale, creando problemi alla sicurezza e all'immagine dell'Ente stesso.

Premesso quindi che l'utilizzo delle risorse informatiche e telematiche dell' **ente** deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro, il **Comune di San Pellegrino Terme** ha adottato un Regolamento interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.

Tali prescrizioni si aggiungono ed integrano le specifiche istruzioni che vanno fornite a tutti gli incaricati in attuazione del D.lgs 196/03 - Testo Unico in materia di protezione dei dati personali.

1. Utilizzo del Personal Computer

1.1 Il Personal Computer affidato al dipendente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione, minacce alla sicurezza e conseguenti responsabilità.

1.2 L'accesso all'elaboratore è protetto da password che deve essere custodita dall'incaricato con la massima diligenza e non divulgata. **Le password devono essere utilizzate per l'accesso alla rete e per l'accesso a qualsiasi applicazione che le preveda.**

Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte del Responsabile del Servizio Sistemi Informativi.

1.3 Il Responsabile del Servizio Sistemi Informativi, per l'espletamento delle funzioni e mansioni assegnate, ha la facoltà in qualunque momento di accedere ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica, anche delegando a terzi con specifico informale mandato, in relazione agli scopi di volta in volta identificati.

1.4 Non è consentito installare autonomamente programmi provenienti dall'esterno senza la preventiva autorizzazione del Responsabile del Servizio Sistemi Informativi ed una richiesta scritta da parte del responsabile dell'unità cui è assegnato il PC.

In caso di necessità di acquisto o dotazione di software applicativi e/o procedure pertinenti esclusivamente ad alcuni settori, deve essere comunque richiesta per iscritto l'autorizzazione preventiva da parte del Responsabile del Servizio Sistemi Informativi, per garantire la compatibilità funzionale, tecnica ed il mantenimento dell'efficienza operativa dei sistemi e delle reti. Sussiste infatti il grave pericolo di introdurre involontariamente virus informatici o di alterare la stabilità delle applicazioni degli elaboratori e dei sistemi operativi.

1.5 Non è consentito l'uso di programmi diversi da quelli distribuiti ufficialmente **dal Servizio Sistemi Informativi del Comune San Pellegrino Terme** (dlg. 518/92 sulla tutela giuridica del software e L. 248/2000 nuove norme di tutela del diritto d'autore).

1.6 Non è consentito all'utente modificare le caratteristiche impostate sui PC assegnati, i punti rete di accesso e le configurazioni delle reti LAN/WAN presenti nelle sedi, salvo autorizzazione esplicita del Responsabile del Servizio Sistemi Informativi.

1.7 E' responsabilità dei responsabili di servizio verificare il coerente utilizzo delle risorse assegnate ed evitarne l'uso improprio o l'accesso alle risorse da parte di personale non autorizzato, compreso l'utilizzo da parte di terzi di punti rete in luoghi non presidiati.

1.8 Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso

di assenze prolungate dall'ufficio. In ogni caso 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. In ogni caso deve essere attivato lo screen saver e la relativa password.

1.9 Non è consentita l'installazione sul proprio PC o il collegamento sulla rete LAN di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, pc portatili ed apparati in genere ...), se non con l'autorizzazione espressa del Responsabile del Servizio Sistemi Informativi, previa richiesta scritta da parte responsabile dell'unità cui è assegnato il PC o il segmento di rete LAN.

1.10 Agli utenti incaricati del trattamento dei dati sensibili è fatto divieto l'accesso contemporaneo con lo stesso account da più PC (art. 5 del DPR 318/99).

E' fatto altresì obbligo di distruggere eventuali copie di sicurezza o supporti di tipo removibile (floppy, CDRom, Nastri) una volta non sia possibile rendere irrecuperabili i dati in essi contenuti.

Ai sensi del Dlgs 196/03 è fatto divieto di divulgazione a qualsiasi titolo delle informazioni presenti nelle banche dati dell'ente se non disciplinate da appositi protocolli di intesa.

1.11 Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente Il Responsabile del Servizio Sistemi Informativi nel caso in cui siano rilevati virus ed adottando quanto previsto dal successivo punto 8 del presente Regolamento relativo alle procedure di protezione antivirus.

1.12 Non è consentita 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.

1.13 E' prevista la progressiva erogazione di tutti servizi di supporto (Help Desk) per le problematiche funzionali di tipo hardware e software, attraverso procedure informatiche centralizzate. Il Servizio Informatico si riserva di non intervenire per anomalie segnalate senza l'utilizzo delle procedure concordate di volta in volta con la Direzione.

2. Utilizzo della rete del Comune di San Pellegrino Terme

2.1 Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità, potranno essere svolte regolari attività di controllo, amministrazione e backup da parte dell'Amministratore del Sistema.

Al fine di garantire la corretta gestione delle politiche di sicurezza delle informazioni è fatto divieto di replicare su dischi locali dei PC dati aziendali, banche dati e documenti sensibili senza esplicita autorizzazione del Responsabile del Servizio Sistemi Informativi e senza l'adozione di adeguate politiche di sicurezza, quali la crittazione dei dati stessi e l'adozione di politiche di backup comprensive della dotazione di idonei archivi protetti.

2.2 Le password d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite. E' assolutamente proibito entrare nella rete e nei programmi con nomi utente diversi dai propri o dal proprio nel caso di accesso univoco. (Global Sign-On).

2.3 Il Responsabile del Servizio Sistemi Informativi può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.

2.4 Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. E' infatti assolutamente da evitare un'archiviazione ridondante.

2.5 E' cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni.

E' buona regola evitare di stampare documenti o file non adatti (molto lunghi o non supportati, come ad esempio il formato pdf o file di contenuto grafico) su stampanti comuni. In caso di necessità la stampa in corso può essere cancellata.

2.6 Non è consentito collegare reti di pc od altri dispositivi alla rete aziendale senza la preventiva autorizzazione scritta dell'Amministratore di Sistema ed una verifica della conformità agli standard tecnici presenti.

3. Gestione delle Password e degli account

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

3.2 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:

- password di rete, per l'avvio e l'utilizzo del sistema operativo e di tutte le risorse di rete
- password per l'accesso a particolari programmi e applicativi.

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

Non è consentita l'attivazione della password d'accensione (bios), senza preventiva autorizzazione da parte della struttura competente.

3.3 Le password d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite.

3.4 E' assolutamente proibito entrare nella rete e nei programmi con nomi utente diversi dai propri o dal proprio nel caso di accesso univoco (global sign on).

3.5 In caso di assenze prolungate e programmate, qualora se ne ravvisi la necessità, il dipendente interessato deve delegare in forma scritta un altro dipendente all'utilizzo del proprio personal computer, comunicandogli le password necessarie e provvedendo, al rientro in ufficio, alla loro sostituzione.

4. Utilizzo dei supporti magnetici

4.1 Tutti i supporti magnetici riutilizzabili (dischetti, cassette, cartucce) contenenti dati sensibili devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato. Una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione.

4.2 I supporti magnetici contenenti dati sensibili devono essere custoditi in archivi chiusi a chiave.

4.3 Non è consentito scaricare files contenuti in supporti magnetici/ ottici non aventi alcuna attinenza con la propria prestazione lavorativa.

4.4 Tutti i files di provenienza incerta, ancorché potenzialmente attinenti all'attività lavorativa, non devono essere utilizzati / installati / testati.

Nel caso di effettiva necessità di impiego devono essere sottoposti ad un preventivo controllo ed alla relativa autorizzazione all'utilizzo da parte del Responsabile del Servizio Sistemi Informativi e/o del suo staff tecnico.

5. Utilizzo di PC portatili

5.1 L'utente è responsabile del PC portatile assegnatogli dall'Amministrazione e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

5.2 Ai PC portatili si applicano le regole di utilizzo previste per i Pc connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.

5.3 I PC portatili utilizzati all'esterno (convegni etc.), in caso di allontanamento, devono essere custoditi in un luogo protetto.

5.4 Eventuali configurazioni di tipo Accesso Remoto, dirette verso la rete aziendale o attraverso internet, devono essere autorizzate esclusivamente a cura del Responsabile del Servizio Sistemi Informativi. E' vietato utilizzare le suddette connessioni all'interno delle sedi comunali se contemporaneamente connessi alla rete LAN.

6. Uso della posta elettronica

6.1 La casella di posta, assegnata all'utente, è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

Si rammenta che i sistemi di posta elettronica non consentono al momento di garantire la riservatezza delle informazioni trasmesse, si raccomandano gli utenti di non inoltrare dati ed informazioni classificabili "sensibili" o "riservate" con questo mezzo.

6.2 E' fatto divieto di utilizzare le caselle di posta elettronica@comune.sanpellegrinoterme.bg.it per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list non attinenti la propria attività o funzione svolta per l'ente.

6.3 E' buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti. E' previsto un dimensionamento massimo per ciascuna casella in relazione alla disponibilità di spazio dei sistemi di posta di volta in volta disponibili, che non potrà essere superato per evitare l'appesantimento della gestione dei server stessi.

6.4 Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali **per il Comune di San Pellegrino Terme** ovvero contenga documenti da considerarsi riservati in quanto contraddistinti dalla dicitura "strettamente riservati" o da analogha dicitura, deve essere visionata od autorizzata dal Dirigente cui si riferisce l'attività ed indirizzata alla casella istituzionale prevista dal Manuale di Gestione del Protocollo Informatico e dei Flussi Documentali.

6.5 E' possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario, ma di norma per la comunicazione ufficiale a privati è obbligatorio avvalersi degli strumenti tradizionali (posta etc. ...) o caselle di posta elettronica certificata, mentre per gli enti pubblici si utilizza il sistema di interoperabilità previsto dal Protocollo Informatico.

. L'amministrazione rende inoltre disponibili anche indirizzi di posta elettronica condivisi da più utenti. Tali indirizzi condivisi devono essere utilizzati esclusivamente per la ricezione di messaggi. Solo in presenza di particolari e specifiche necessità, (esempio caselle di posta elettronica certificata) e previa autorizzazione della struttura competente le caselle di posta elettronica condivisa potranno essere utilizzate per l'invio di messaggi o trasmissione di file.

6.6 Per la trasmissione di file all'interno del **Comune di San Pellegrino Terme** è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati, se di dimensioni consistenti si consiglia di utilizzare le directory di scambio presenti sui file server, notificando a mezzo mail al destinatario la disponibilità del file stesso.

6.7 E' obbligatorio controllare con il Sw antivirus i files attachments di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

6.8 E' vietato inviare catene telematiche (o di Sant'Antonio). Se si dovessero ricevere messaggi di tale tipo, si deve comunicarlo immediatamente all'Amministratore del Sistema. Non si deve in alcun caso attivare gli allegati di tali messaggi.

7. Uso della rete Internet e dei relativi servizi

7.1 Il PC abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa. E' proibita la navigazione in Internet per motivi diversi da quelli funzionali all'attività lavorativa stessa.

7.2 E' fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dal Responsabile del Servizio.

7.3 E' tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati o attinenti i compiti e le mansioni assegnate e con il rispetto delle normali procedure di acquisto.

7.4 E' da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.

7.5 E' vietata la partecipazione a Forum non professionali, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames), se non attinenti l'attività lavorativa svolta.

7.6 Il Servizio Sistemi Informativi si riserva di applicare per singoli e gruppi di utenti politiche di navigazione personalizzate in base alle mansioni ed eventuali disposizioni concordate al fine di ottimizzare l'uso delle risorse, gli investimenti e le prestazioni delle connessioni esistenti.

7.7 Non è consentita la navigazione in siti ove sia possibile rivelare le opinioni politiche, religiose o sindacali dell'utilizzatore; non è consentito inoltre visitare siti e memorizzare documenti informatici dai contenuti di natura oltraggiosa e/o discriminatoria per sesso/etnia/religione/opinione e/o appartenenza sindacale e/o politica.

8. Protezione antivirus

8.1 Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo.

8.2 Ogni utente è tenuto a controllare il regolare funzionamento e l'aggiornamento periodico del software installato, secondo le procedure previste.

8.3 Nel caso che il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente: a) sospendere ogni elaborazione in corso **senza spegnere il computer** b) segnalare l'accaduto al Responsabile del Servizio Sistemi Informativi.

8.4 Non è consentito l'utilizzo di floppy disk, cd rom, cd riscrivibili, supporti magnetici di provenienza ignota.

8.5 Ogni dispositivo magnetico di provenienza esterna all'azienda dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere consegnato all'amministratore di sistema.

9. Osservanza delle disposizioni in materia di Privacy

9.1 E' obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza. Tale norma andrà indicata nelle lettere di individuazione dell'incaricato al trattamento dei dati ai sensi del D.lgs 196/03.

10. Controlli e responsabilità

10.1 L'Amministrazione si riserva di effettuare controlli sul corretto utilizzo degli strumenti informatici e telematici nel rispetto delle normative vigenti e del presente regolamento.

10.2 Per esigenze organizzative, produttive e di sicurezza l'Amministrazione può avvalersi di strumenti che consentono un controllo a distanza relativo all'intera struttura amministrativa, ad aree, settori o gruppi di utenti. Le irregolarità e anomalie rilevate verranno immediatamente contestate ai responsabili.

10.3 Nei casi più gravi il mancato rispetto o la violazione delle norme contenute nel presente regolamento verrà perseguito oltre che con provvedimenti disciplinari, con le azioni civili e penali previste dalle norme vigenti.

11. Entrata in vigore

11.1 Il presente Regolamento entra in vigore con l'approvazione del Consiglio Comunale.

ALLEGATO A

GLOSSARIO DEI TERMINI TECNICI E INFORMATICI

Account	Iscrizione registrata su un server e che, tramite l'inserimento di una userId 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.