Unione Comuni Garfagnana

LOCO ET TEMPORE

GARFAGNANA

UTILIZZO DEGLI STRUMENTI INFORMATICI, DEI SERVIZI DI TELEFONIA E MODALITA' DI CONTROLLO

REGOLAMENTO

(Redatto tenendo conto delle linee guida del Garante della Privacy, emanate con delibera n. 13 del 1° marzo 2007)

Approvato con Deliberazione del Consiglio dell' Unione Comuni n° 10 del 29.04.2013

INDICE

CAPO I
FINALITA' - AMBITO DI APPLICAZIONE — PRINCIPI GENERALI

Art. 1 – Finalità ed ambito di applicazione

1. Il presente Regolamento:

a. definisce le modalità di accesso e di corretto utilizzo degli strumenti informatici, di internet, della posta elettronica, e dei servizi di telefonia dell' Unione Comuni Garfagnana;

b. si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello; a tutti i collaboratori dell' Unione Comuni, a prescindere dal rapporto contrattuale con la stessa intrattenuto; a tutti gli amministratori. Tali soggetti sono nel prosieguo definiti utenti.

2. Gli strumenti informatici sono costituiti dall'insieme delle risorse informatiche dell'Ente, sia infrastrutturali (hardware e software) che informativo-digitali (banche dati in formato digitale e, in generale, tutti i documenti prodotti tramite l'utilizzo delle risorse infrastrutturali).

3. I servizi di telefonia sono costituiti dall'insieme delle infrastrutture telefoniche in dotazione, in particolare dalle linee e dagli apparecchi telefonici, cellulari compresi.

4. L'Ente promuove ogni opportuna misura, formativa, organizzativa e tecnologica, volta a prevenire il rischio di utilizzi impropri delle strumentazioni e delle banche dati di proprietà e disciplina le modalità con cui effettuerà i relativi controlli.

Art. 2 - Princìpi generali

1. L' Unione Comuni Garfagnana promuove, nel rispetto delle linee guida e dei princìpi della normativa vigente, l'utilizzo degli apparati telefonici ed informatici, di internet e della posta elettronica, in quanto mezzi utili a perseguire con efficacia ed efficienza le proprie finalità istituzionali.

2. Ogni utente è responsabile, civilmente e penalmente, del corretto uso delle risorse informatiche e telefoniche assegnate e del contenuto delle comunicazioni effettuate e ricevute, 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.

CAPO II
GESTIONE DEGLI STRUMENTI INFORMATICI E TELEFONICI

Art. 3 - Modalità di utilizzo degli strumenti informatici

1. Il personal computer (fisso o portatile) è uno strumento di lavoro individuale, che non può essere ceduto a terzi, estranei all'Ente. L'utente ne è responsabile e deve custodirlo con diligenza, sia presso il proprio ufficio, che durante gli spostamenti (portatile), adottando tutti gli accorgimenti necessari ad evitare danni o sottrazioni. Ogni utilizzo non inerente all'attività lavorativa è vietato, perché può contribuire ad innescare disservizi, aumentare i costi di manutenzione e, soprattutto, minacciare la sicurezza.

2. Nell'espletamento della propria attività lavorativa, gli utenti non devono:

a. usare programmi diversi da quelli installati dal personale della ditta incaricata della manutenzione e gestione dell'hardware, del software e della rete dell'Ente (nel prosieguo, per brevità, Servizio ICT) e modificare la configurazione del proprio personal computer;

b. scaricare e/o installare programmi e file, anche gratuiti, da siti internet e copiare file di provenienza incerta, da supporti quali pen drive, Cd-ROM, DVD, ecc., se non previa verifica del Servizio ICT, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esi-

stenti. L'inosservanza della presente disposizione espone la stessa Unione Comuni a gravi responsabilità civili;

c. installare software privo di licenza d'uso. La violazione della normativa a tutela dei diritti d'autore prevede pesanti sanzioni pecuniarie ed interdittive e può anche comportare una responsabilità amministrativa a carico dell' Unione Comuni, come disposto dall'art. 25-nonies del D.lgs. 8 giugno 2001, n° 231;

d. installare periferiche (hard-disk, DVD, fotocamere, apparati multimediali, masterizzatori, modem, ecc.) esterne agli strumenti in dotazione, se non per esigenze di servizio, se non previa verifica del Servizio ICT;

e. consultare, memorizzare e diffondere documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;

f. duplicare e/o cedere programmi e altro materiale informatico, se non nelle forme e per gli scopi di servizio per i quali sono stati assegnati;

devono invece:

a. utilizzare gli applicativi gestionali, destinati al trattamento di informazioni, in maniera compatibile con la vigente normativa sulla privacy (D.lgs. n° 196/2003 e successive modificazioni);

b. comunicare tempestivamente al Servizio ICT l'eventuale malfunzionamento o danneggiamento del pc;

c. effettuare il back-up, su hard disk esterno, dei dati presenti sulle proprie unità di memorizzazione locali (es. HD interno del pc), evitando comunque un'archiviazione ridondante;

d. spegnere il personal computer ogni sera prima di lasciare l'ufficio. In ogni caso, per assenze prolungate dalla propria postazione di lavoro, l'utente dovrà, prima di tutto, procedere a chiudere ogni applicazione attiva e bloccare l'accesso al computer (utilizzo di salvaschermo dotato di password; eventuale estrazione e custodia dell'hardware di autenticazione e degli altri supporti rimovibili; ecc.). Lasciare un pc 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.

Art. 4 - Utilizzo condiviso delle periferiche e delle cartelle

1. Per periferica condivisa si intende qualsiasi dispositivo elettronico (stampanti, scanner, plotter, ecc.), che può essere utilizzato in contemporanea da più uffici.

2. Per cartella condivisa (unità di rete) si intende uno spazio disco disponibile sui server, client ed hard disk esterni, per la memorizzazione di dati e programmi accessibili ad un gruppo di utenti, preventivamente autorizzati.

3. L'utente è tenuto ad utilizzare le unità di rete esclusivamente per la condivisione di informazioni istituzionali; non può pertanto collocare in queste aree, anche temporaneamente, file non attinenti all'attività lavorativa. Stessa cosa dicasi per l'utilizzo delle periferiche e dei materiali di consumo in genere (carta, inchiostro, toner, supporti magnetici, supporti digitali), con in più l'accortezza di evitare sprechi od utilizzi eccessivi.

4. I Dirigenti si impegnano ad eliminare, ove possibile, le stampanti e/o gli scanner personali, in favore di quelli di rete, che permettono un risparmio nei costi di gestione.

Art. 5 - Utilizzo e conservazione dei supporti rimovibili

1. Tutti i supporti magnetici rimovibili (floppy disk, CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati sensibili nonché informazioni costituenti know-how dell'Ente, devono essere trattati con particolare cautela, onde evitare che il loro contenuto possa essere trafugato, alterato, distrutto o, successivamente alla cancellazione, recuperato. In quest'ultimo caso, ciascun utente dovrà contattare il personale del Servizio ICT ed attenersi alle indicazioni da questo impartite.

2. L'utente è responsabile della custodia dei supporti e dei dati aziendali in essi contenuti che, se sensibili, devono essere conservati in armadi chiusi.
3. E' vietato l'utilizzo di supporti rimovibili personali (non forniti dall'Ente).

Art. 6 - Utilizzo dei servizi e degli apparecchi telefonici fissi e mobili

1. I telefoni dell' Unione Comuni (fissi e cellulari) sono esclusivamente uno strumento di lavoro. Non sono pertanto consentite comunicazioni o invio/ricezione di messaggi a carattere personale o non strettamente inerenti l'attività lavorativa. L'assegnatario è responsabile del loro utilizzo e custodia.
2. L'utilizzo promiscuo è consentito solo in presenza di specifica disposizione dell'Ente, che ne preciserà anche le modalità.

3. Al fine di garantire un migliore utilizzo dei servizi di telefonia, l' Unione Comuni predispone adeguate profilazioni, che consentano l'effettuazione di parte o dell'intera tipologia di chiamate.

4. E' fatto assoluto divieto di cessione a terzi degli apparecchi e delle SIM.

5. Se le condizioni di ricezione del segnale lo consentono, quando gli assegnatari sono in servizio, i cellulari devono risultare attivi e raggiungibili.

Art. 7 - Gestione delle password e degli account

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

2. Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dal personale del Servizio ICT, previa formale richiesta del Dirigente nella cui area andrà ad operare il nuovo utente.

3. Si distinguono account di accesso alla rete (avvio ed utilizzo del sistema operativo e di tutte le risorse di rete) ed ai programmi ed applicativi autorizzati.

4. La password, formata da lettere (maiuscole o minuscole) e/o numeri, anche in combinazione fra loro, deve essere composta da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'utente. Deve essere modificata al primo utilizzo e, periodicamente, almeno ogni sei mesi (ogni tre mesi nel caso di trattamento di dati sensibili attraverso l'ausilio di strumenti elettronici), secondo la procedura proposta automaticamente all'utente.

5. La password è personale e segreta. Pertanto deve essere nota solo all'utente, che è responsabile, civilmente e penalmente, della custodia e della segretezza delle proprie credenziali (D.lgs. n° 196/2003 e s.m.i.).

6. Con la cessazione del rapporto di lavoro, l'account individuale dell'utente verrà immediatamente dismesso.

7. E' compito del Servizio Personale aggiornare tempestivamente le variazioni degli utenti sulla intranet, in modo che il Servizio ICT possa procedere alla creazione, modifica e cancellazione degli account.

8. Soggetto preposto alla custodia delle credenziali di autenticazione è il personale del Servizio ICT.

Art. 8 - Protezione antivirus

1. Il sistema informatico dell' Unione Comuni è protetto da software antivirus, aggiornato quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacchi (art. 3 comma 2; art. 11 commi 3 e 4).

2. Qualora venga rilevata la presenza di un virus, l'utente dovrà segnalarlo immediatamente al personale del Servizio ICT, sospendendo ogni elaborazione in corso, senza spegnere il computer.

3. Ogni dispositivo magnetico di provenienza esterna all'Ente, prima del suo utilizzo, dovrà essere monitorato con il programma antivirus. In caso di infezione, l'utente dovrà procedere come al precedente punto 2.

CAPO III
GESTIONE DELLE COMUNICAZIONI TELEMATICHE

Art. 9 - Utilizzo di Internet

1. Ferme restando le modalità di utilizzo degli strumenti informatici di cui all'art. 3, agli utenti è vietato utilizzare internet per attività non strettamente attinenti allo svolgimento delle mansioni assegnate ed in particolare:

a. accedere e/o registrarsi a siti, specialmente se con contenuti non adeguati alla serietà ed al decoro richiesti nei luoghi di lavoro; consultare banche dati a pagamento (ad esempio, SISTER, SIATEL, ecc...);

b. effettuare transazioni finanziarie, ivi comprese operazioni di remote banking, acquisti on-line e simili; partecipare a forum non istituzionali ed utilizzare chat line, bacheche elettroniche, social network (ad esempio, Facebook), guest books, anche utilizzando pseudonimi (nicknames);

c. scambiare materiale protetto dalla normativa vigente in tema di tutela del diritto d'autore ed utilizzare sistemi di scambio dati/informazioni con tecnologie "peer to peer";

d. accedere a caselle web mail di posta elettronica personale; effettuare l'upload od il download di software gratuiti (freeware) e shareware, nonché utilizzare documenti provenienti da siti web o http (filmati e musica).

2. L'Amministrazione si riserva di adottare uno specifico sistema di blocco o filtro automatico (c.d. "black list"), così da applicare profili di navigazione personalizzati per aree o servizi, correlati con l'attività lavorativa svolta.

Art. 10 - Utilizzo della rete dell' Unione Comuni

1. Per l'accesso alla rete dell' Unione Comuni, ciascun utente deve essere in possesso della specifica credenziale di autenticazione, che è personale e segreta (art. 7 comma 5).

2. È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione diverso da quello assegnato.

3. E' opportuno che, almeno ogni tre mesi, ciascun utente provveda alla pulizia dei propri archivi (cancellazione dei file inutilizzati) ed al back up dei dati, evitando comunque un'archiviazione ridondante.

Art. 11 - Gestione ed utilizzo della posta elettronica

1. La posta elettronica è uno strumento di lavoro e ciascun assegnatario:

a. è responsabile del corretto utilizzo della stessa;

b. deve assicurare quotidianamente la lettura e l'evasione delle e-mail ricevute;

c. deve mantenere in ordine la propria casella, cancellando documenti inutili e, soprattutto, allegati ingombranti.

2. La gestione delle caselle e-mail avviene in modo centralizzato su server e l'accesso si realizza mediante l'utilizzo di client di posta elettronica installati localmente.

3. E' vietato utilizzare le caselle di posta elettronica per motivi diversi da quelli strettamente legati all'attività lavorativa quali, a puro titolo esemplificativo:

a. Inoltro di "mail spamming", appelli e petizioni, giochi, scherzi e barzellette, "catene di Sant'Antonio" (in caso di ricezione di tale tipologia di messaggio, dovrà essere immediatamente informato il personale del Servizio ICT e non si dovrà in alcun caso procedere all'apertura degli eventuali allegati), ecc.;

b. Trasmissione dolosa di virus, worms, trojan o altro codice maligno, finalizzati ad arrecare danni e malfunzionamenti ai sistemi informatici;

c. Invio o ricevimento di allegati contenenti filmati o brani musicali (es. mp3) non legati all'attività lavorativa;

d. Invio o ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list.

4. È obbligatorio porre la massima attenzione nell'aprire i file attachements di posta elettronica (non eseguire il download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

5. AI fine di garantire la funzionalità del servizio di posta elettronica aziendale e di ridurre al minimo l'accesso ai dati, nel rispetto del principio di necessità e proporzionalità, in caso di assenze programmate (ad es. per ferie od attività di lavoro fuori sede), l'assegnatario della casella dovrà attivare un'apposita funzionalità del sistema, la quale invierà automaticamente ai mittenti messaggi di risposta contenenti le "coordinate" di posta elettronica di un collega o altre modalità per contattare la struttura. Qualora l'utente, per dimenticanza o per assenza non programmata (malattia, ecc.), non possa attivare tale procedura entro due giorni, verrà surrogato dal proprio Dirigente, attraverso il Servizio ICT, che può comunque procedere d'ufficio nei casi di estrema urgenza, informato il Dirigente CED.

6. Ogni comunicazione inviata o ricevuta, che abbia contenuti rilevanti, documenti riservati (dicitura "strettamente riservato" o simile), impegni contrattuali/precontrattuali, deve essere, rispettivamente, autorizzata o visionata dal Dirigente della struttura.

7. AI fine di ribadire agli interlocutori la natura esclusivamente aziendale della casella di posta elettronica, i messaggi devono contenere un avvertimento standardizzato, nel quale sia dichiarata la natura non personale dei messaggi stessi e, pertanto, la possibilità che il personale incaricato dell' Unione Comuni possa accedere, secondo le regole fissate nella policy dell'Ente, al contenuto del messaggio inviato.

8. In caso di cessazione del rapporto di lavoro, la casella di posta elettronica individuale dell'utente verrà immediatamente dismessa.

CAPO IV
ASSISTENZA, CONTROLLO E SANZIONI

Art. 12 – Assistenza, controlli, responsabilità e sanzioni

1. Le richieste di assistenza e servizi avvengono per chiamata diretta del Servizio ICT, al numero interno 344, che le gestisce in base alla cronologia ed all'urgenza.

2. L' Unione Comuni rende noto che, nel rispetto della normativa sulla privacy ed in coerenza con il punto 3. della deliberazione dell'Autorità Garante per la protezione dei dati personali 1 marzo 2007, n° 13 e quindi per finalità del tutto estranee al controllo dell'attività lavorativa, il personale del Servizio ICT è autorizzato a:

a. compiere interventi sul sistema informatico dell'Ente e sulle singole postazioni lavorative, per garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento, sostituzione od implementazione di programmi, manutenzione hardware, etc.).

b. collegarsi e visualizzare in remoto il desktop delle singole postazioni PC, al fine di garantire l'assistenza tecnica e la normale attività operativa, nonché la massima sicurezza contro virus, spyware, malware, etc. L'intervento viene effettuato sia su chiamata dell'utente che in casi di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico.

c. registrare e conservare, per il tempo strettamente necessario, i tabulati del traffico telefonico, con l'oscuramento delle ultime tre cifre delle numerazioni.

d. disporre controlli a campione sui siti web visitati (ricerca di eventuali errori, controllo della sicurezza del sistema, verifica di eventuali abusi). L'accesso ai dati di connessione, che comprendono data e ora, indirizzo IP di mittente e destinatario, volume complessivo dei dati trasmessi, avverrà mediante un sistema di controllo dei contenuti (Proxy server) o mediante "file di log" della navigazione svolta. I file verranno conservati non oltre 12 mesi, tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dell'Ente.

e. effettuare attività di controllo, amministrazione e back up sulle cartelle utenti, presenti nei server.

f. procedere alla rimozione di file od applicazioni ritenuti pericolosi per la sicurezza, sia sulle unità di rete che sui singoli pc.

g. accedere alle varie caselle di posta elettronica;

3. Sono invece escluse, al di là di quanto tecnicamente necessario per svolgere il servizio di cui al precedente punto 1., attività sistematiche di:

- lettura e registrazione dei messaggi di posta elettronica ovvero dei relativi dati esteriori;
- riproduzione ed eventuale memorizzazione delle pagine web visualizzate;
- lettura e registrazione dei caratteri inseriti tramite tastiera o analogo dispositivo;
- analisi di computer da remoto.

4. Qualora, in tali attività, vengano rilevate anomalie nell'utilizzo degli strumenti informatici e telefonici, l'Amministrazione procederà preliminarmente all'invio di un avviso generalizzato agli utenti dell'area o del settore in cui e stata rilevata l'anomalia, nel quale si evidenzierà l'utilizzo irregolare degli strumenti aziendali e si inviteranno gli interessati ad attenersi scrupolosamente al presente Regolamento ed alla normativa vigente. Controlli su base individuale saranno compiuti solo in caso di successive ulteriori anomalie.

5. Il mancato rispetto delle regole di cui sopra è perseguibile con provvedimenti disciplinari e/o risarcitori, previsti dal vigente CCNL del personale, dirigente e non, del comparto Regioni ed Autonomie locali, nonché con tutte le azioni civili e penali consentite, previo espletamento di apposito procedimento (disciplinare, ecc.).

CAPO V
NORME FINALI

Art. 13 - Formazione e aggiornamento

1. L' Unione Comuni promuove, all'interno del proprio piano annuale della formazione, corsi inerenti le materie del presente Regolamento.

Art. 14 - Entrata in vigore e revisione del Regolamento

1. Il presente Regolamento entrerà in vigore il 20.06.2013 e, da tale data, tutte le disposizioni in precedenza adottate in materia, devono intendersi abrogate e sostituite dalle presenti.

2. Il presente Regolamento è soggetto, di norma, a revisione biennale. Gli utenti possono proporre integrazioni e modifiche motivate.

ALLEGATO A : Presa visione ed accettazione del Regolamento

Il/La sottoscritto/a …….. nato/a …….. il ……,

residente a …….. in via …… n° ……., Telefono ……,

cod. fisc. ……

Dichiara di:

- aver ricevuto copia, aver preso visione ed accettare tutte le norme contenute nel Regolamento;
- aver acquisito le informazioni di cui all'art. 13 del D.lgs n° 196 del 30 Giugno 2003;
- essere a conoscenza dei diritti dell'interessato, di cui agli articoli 7, 8, 9, 10, del medesimo decreto.

Data ……..

Firma ……..

ALLEGATO B : Glossario dei termini tecnici ed informatici

Account	Iscrizione registrata su un server e che, tramite l'inserimento di una user id 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 gli stessi virus hanno compiuto.
Backup	Backup Copia di riserva di disco, di una parte del disco o di uno o più file.
Black list	Elenco di siti considerati non opportuni per l'espletamento delle funzioni lavorative dell'Amministrazione.
Database	Database (Base di Dati). Qualsiasi aggregato di dati organizzato in campo (colonne) e record (righe).
Download	Download Registrare sul proprio disco rigido un file richiamandolo, tramite modem 0 rete, da un computer, da un server o da un host (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	Freeware Software gratuito realizzato e distribuito da privati o piccole società, attraverso Internet o CD—ROM allegati a pubblicazioni in edicola.
Hardware	Hardware Letteralmente ferramenta, in informatica si intende l'insieme dei componenti (CPU, Hard Disk ecc.) che costituiscono un computer.
Service desk	Service Desk Risorsa informativa e di assistenza che prende in carico i problemi che sorgono nell'uso del sistema informativo comunale.
Internet	La madre di tutte le reti di computer. E' l'insieme mondiale delle reti di computer interconnesse.
Intranet	La Intranet e una rete locale (Local Area Network), o un raggruppamento di reti locali, usata all'interno di una organizzazione per facilitare la comunicazione e l'accesso alle informazioni.
MP3 (MPEG-4)	MP3 (MPEG-4) Tecnologia per la compressione/decompressione di file audio/video che consente di mantenere una perfetta fedeltà e qualità anche riducendo i file di ben 11 volte la grandezza originale.
MPG (Motion Picture Experts Group)	MPG (Motion Picture Stabilisce gli standard digitali per audio e video. E' in particolare lo Experts Group) standard di compressione utilizzato per codificare i video registrati su DVD.
Password	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 (caratteri maiuscoli/minuscoli), assieme alla user-id.
Quicktime	Standard definito dalla Apple e utilizzato da tutti i computer per la riproduzione fedele dei filmati video.
SIC	Sistemi Informativi Comunali — Servizio che, nell'ambito dell'Amministrazione, si occupa di impostare, indirizzare e coordinare l'introduzione delle tecnologie informatiche nell'attività del Comune, ponendosi quale punto di riferimento tecnologico per la definizione delle strategie di evoluzione e innovazione dei Sistemi Informativi.
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.
White list	Elenco di siti considerati opportuni per l'espletamento delle funzioni lavorative dell'Amministrazione.