



Trento, 10 settembre 2007

CIRCOLARE N°38/2007

GF/lb

Agli Enti Soci

- LL.SS. -

OGGETTO: Linee guida del Garante per la protezione dei dati personali per posta elettronica e internet – Provvedimento generale 1 marzo 2007.

Indicazioni e prescrizioni – modello di disciplinare interno.

Riportiamo di seguito la circolare elaborata dal dott. Gianni Festi, dello sportello di consulenza in materia di privacy, dello scrivente Consorzio dei Comuni Trentini.

INDICAZIONI E PRESCRIZIONI

Con riferimento alla precedente circolare n. 24 dd. 8 giugno 2007, si forniscono di seguito **indicazioni e chiarimenti** in merito agli adempimenti da compiersi da parte dei Comuni ai fini del corretto utilizzo da parte dei propri dipendenti di internet e della posta elettronica e dell'eventuale legittimo controllo di tale attività da parte del Comune.

Con il provvedimento di cui in oggetto il Garante per la protezione dei dati personali ha prescritto ai datori di lavoro privati e pubblici, ai sensi dell'art. 154, comma 1, lett. c), del Codice in materia di protezione di dati personali, di adottare la misura necessaria riguardante l'onere di specificare le modalità di utilizzo della posta elettronica e della rete Internet da parte dei lavoratori, indicando chiaramente le modalità di uso degli strumenti messi a disposizione e se, in che misura e con quali modalità vengano effettuati controlli;



1. Adozione e pubblicizzazione di un disciplinare interno

Il Comune deve indicare, chiaramente e in modo particolareggiato, **quali siano le modalità di utilizzo degli strumenti messi a disposizione ritenute corrette e se, in che misura e con quali modalità vengano effettuati controlli.**

Il disciplinare interno deve specificare tali modalità e eventuali possibilità controllo e, più in generale, la policy aziendale del Comune e deve essere **adeguatamente pubblicizzato** (mediante consegna ai singoli lavoratori, nella rete interna, mediante affissioni sui luoghi di lavoro con modalità analoghe a quelle previste dall'art. 7 dello Statuto dei lavoratori, ecc.).

Deve in particolare specificare, in relazione alle proprie scelte organizzative:

- se determinati comportamenti non sono tollerati rispetto alla "navigazione" in Internet (ad es. il download di software o di file musicali), oppure alla tenuta di file nella rete interna;
- in quale misura è consentito utilizzare anche per ragioni personali servizi di posta elettronica o di rete, anche solo da determinate postazioni di lavoro o caselle oppure ricorrendo a sistemi di webmail, indicandone le modalità e l'arco temporale di utilizzo (ad es. fuori dall'orario di lavoro o durante le pause, o consentendone un uso moderato anche nel tempo di lavoro);
- quali informazioni sono memorizzate temporaneamente (ad es. le componenti di file di log eventualmente registrati) e chi (anche all'esterno) vi può accedere legittimamente;
- se e quali informazioni sono eventualmente conservate per un periodo più lungo, in forma centralizzata o meno (anche per effetto di copie di back up, della gestione tecnica della rete o di file di log);
- se, e in quale misura, il Comune si riserva di effettuare controlli in conformità alla legge, anche saltuari o occasionali, indicando le ragioni legittime, specifiche e non generiche, per cui verrebbero effettuati (anche per verifiche sulla funzionalità e sicurezza del sistema) e le relative modalità (precisando se, in caso di abusi singoli o reiterati, vengono inoltrati preventivi avvisi collettivi o individuali ed effettuati controlli nominativi o su singoli dispositivi e postazioni);
- quali conseguenze, anche di tipo disciplinare, il Comune si riserva di trarre qualora constatati che la posta elettronica e la rete Internet sono utilizzate indebitamente;
- le soluzioni prefigurate per garantire, con la cooperazione del lavoratore, la continuità dell'attività lavorativa in caso di assenza del lavoratore stesso (specie se programmata), con particolare riferimento all'attivazione di sistemi di risposta automatica ai messaggi di posta elettronica ricevuti;
- se sono utilizzabili modalità di uso personale di mezzi con pagamento o fatturazione a



carico dell'interessato;

- quali misure sono adottate per particolari realtà lavorative nelle quali debba essere rispettato l'eventuale segreto professionale cui siano tenute specifiche figure professionali;
- le prescrizioni interne sulla sicurezza dei dati e dei sistemi (art. 34 del Codice, nonché Allegato B), in particolare regole 4, 9, 10).

2. Adozione di misure di tipo tecnologico

a) Rispetto all'utilizzo di internet

Il Comune deve individuare a quali lavoratori consentire tale utilizzo.

Al fine di ridurre il rischio di usi impropri della "navigazione" in Internet (consistenti in attività non correlate alla prestazione lavorativa quali la visione di siti non pertinenti, o con finalità ludiche o estranee all'attività), deve adottare opportune misure che possono, così, prevenire controlli successivi sul lavoratore, quali:

- individuare categorie di siti considerati correlati o meno con la prestazione lavorativa;
- configurare i sistemi o l'utilizzo di filtri che prevengano determinate operazioni, –reputate inconferenti con l'attività lavorativa, quali l'upload o l'accesso a determinati siti (inseriti in una sorta di black list) e/o il download di file o software aventi particolari caratteristiche (dimensionali o di tipologia di dato);
- trattare i dati in forma anonima o tale da precludere l'immediata identificazione di utenti mediante loro opportune aggregazioni (ad es. con riguardo ai file di log riferiti al traffico web, su base collettiva o per gruppi sufficientemente ampi di lavoratori);
- conservare i dati per il tempo strettamente necessario al perseguimento di finalità organizzative, produttive e di sicurezza.

b) Rispetto all'utilizzo della posta elettronica

Il contenuto dei messaggi di posta elettronica, come pure i dati esteriori delle comunicazioni e i file allegati, sono forme di corrispondenza assistite da garanzie di segretezza, tutelate anche costituzionalmente.

Con riferimento all'impiego della posta elettronica nel contesto lavorativo e in ragione della veste esteriore attribuita all'indirizzo di posta elettronica nei singoli casi, può risultare dubbio se il lavoratore, in qualità di destinatario o mittente, utilizzi la posta elettronica per finalità di servizio o ne faccia un uso personale.

La mancata esplicitazione di una policy al riguardo può determinare anche una legittima aspettativa del lavoratore, o di terzi, di confidenzialità rispetto ad alcune forme di



comunicazione.

È quindi particolarmente opportuno che si adottino accorgimenti che chiariscano quale sia l'utilizzo consentito della posta elettronica

Il Comune deve:

- valutare se rendere disponibili indirizzi di posta elettronica condivisi tra più lavoratori;
- valutare se attribuire al lavoratore un diverso indirizzo destinato ad uso privato del lavoratore;
- mettere a disposizione di ciascun lavoratore apposite funzionalità di sistema, di agevole utilizzo, che consentano di inviare automaticamente, in caso di assenze (ad es., per ferie o attività di lavoro fuori sede), messaggi di risposta contenenti le "coordinate" (anche elettroniche o telefoniche) di un altro soggetto o altre utili modalità di contatto della struttura. È parimenti opportuno prescrivere ai lavoratori di avvalersi di tali modalità, prevenendo così l'apertura della posta elettronica. In caso di eventuali assenze non programmate (ad es., per malattia), qualora il lavoratore non possa attivare la procedura descritta (anche avvalendosi di servizi webmail), il titolare del trattamento, perdurando l'assenza oltre un determinato limite temporale, può disporre lecitamente, sempre che sia necessario e mediante personale appositamente incaricato (ad es. l'amministratore di sistema), l'attivazione di un analogo accorgimento, avvertendo gli interessati;
- in previsione della possibilità che, in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica, adottare una misura che consenta all'interessato di delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. A cura del titolare del trattamento, di tale attività dovrebbe essere redatto apposito verbale e informato il lavoratore interessato alla prima occasione utile;
- adottare una misura per cui i messaggi di posta elettronica contengano un avvertimento ai destinatari nel quale sia dichiarata l'eventuale natura non personale dei messaggi stessi, precisando se le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente e con eventuale rinvio alla predetta policy datoriale.

3. Attività di controllo

Il Comune deve decidere se effettuare attività di controllo.

L'eventuale controllo è lecito solo se sono rispettati i principi di pertinenza e non eccedenza.

Deve essere per quanto possibile preferito un controllo preliminare su dati aggregati, riferiti



all'intera struttura lavorativa o a sue aree.

Il controllo anonimo può concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite. L'avviso può essere circoscritto a dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia. In assenza di successive anomalie non è di regola giustificato effettuare controlli su base individuale.

Non sono legittimi controlli prolungati, costanti o indiscriminati.

I sistemi software devono essere programmati e configurati in modo da cancellare periodicamente ed automaticamente (attraverso procedure di sovraregistrazione come, ad esempio, la cd. rotazione dei log file) i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria.

In assenza di particolari esigenze tecniche o di sicurezza, la conservazione temporanea dei dati relativi all'uso degli strumenti elettronici deve essere giustificata da una finalità specifica e comprovata e limitata al tempo necessario.

Un eventuale prolungamento dei tempi di conservazione va valutato come eccezionale e può aver luogo solo in relazione:

- ad esigenze tecniche o di sicurezza del tutto particolari;
- all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
- all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

Vige l'assoluto divieto di effettuare controlli con le seguenti modalità:

- la lettura e la registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail;
- la riproduzione e l'eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;
- la lettura e la registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
- l'analisi occulta di computer portatili affidati in uso;

MODELLO DI DISCIPLINARE INTERNO

L'allegato modello di disciplinare interno "Criteri e modalità operative per l'accesso e l'utilizzo dei servizi internet e di posta elettronica" costituisce **esclusivamente uno schema-base** che si è ritenuto utile fornire ai comuni ai fini di elaborare e predisporre un proprio disciplinare interno.

Il modello contiene gli elementi che, in osservanza di quanto prescritto dal Provvedimento generale del Garante per la protezione dei dati personali del 1 marzo 2007, devono essere



previsti e specificati da parte del datore di lavoro per il legittimo uso dei servizi internet e di posta elettronica da parte dei propri dipendenti e per il controllo di tale attività da parte del datore di lavoro stesso.

Traendo spunto dall'allegato modello, è necessario elaborare e adottare un disciplinare interno in ragione della propria organizzazione, delle proprie scelte di policy aziendale in materia nonché degli strumenti a disposizione.

Lo stesso dovrà essere oggetto di illustrazione con le rappresentanze sindacali.

In merito alla forma giuridica si ritiene che lo stesso un atto di gestione, di competenza dell'organo tecnico-amministrativo.

Nulla osta chiaramente a che lo stesso, per opportunità, sia sottoposto all'illustrazione della Giunta comunale.

dott. Gianni Festi

Ricordiamo che gli uffici del Consorzio sono a disposizione per ogni chiarimento che dovesse rendersi necessario.

Cordiali saluti.

Il Direttore
dott. Alessandro Ceschi

Il Presidente
dott. Renzo Anderle

All.

Criteria e modalità operative per l'accesso e l'utilizzo del servizio Internet e del servizio di posta elettronica

Informativa ai sensi dell'art. 13 del D.Lgs. 196/2003.

OGGETTO

Il disciplinare, adottato sulla base e secondo le indicazioni contenute nella deliberazione 1 marzo 2007 n. 13 del Garante per la protezione dei dati personali, recante "Linee guida del Garante per posta elettronica e internet", ha per oggetto i criteri e le modalità operative di accesso e utilizzo del servizio internet e di posta elettronica da parte dei dipendenti del Comune di _____ e di tutti gli altri soggetti che a vario titolo prestano servizio o attività per conto e nelle strutture del Comune di _____ (lavoratori socialmente utili, collaboratori, tirocinanti/stagisti).

DEFINIZIONI

Nel presente documento il termine:

- UTENTE INTERNET (BASE): persona autorizzata ad accedere alla lista di siti istituzionali preventivamente selezionati dal Comune;
- UTENTE INTERNET (AMPIO): persona autorizzata ad accedere al servizio internet al di là dei siti istituzionali preventivamente selezionati dal Comune, con l'unico limite di filtri predeterminati che si attivano in modo automatico durante la navigazione;
- UTENTE DI POSTA ELETTRONICA: persona autorizzata ad accedere al servizio di posta elettronica;
- WHITE LIST: elenco di siti direttamente e immediatamente accessibili da tutti gli utenti internet (base)
- BLACK LIST: elenco di siti non accessibili da nessun utente
- INTERNET PROVIDER: azienda che fornisce al Comune il canale di accesso alla rete internet;
- POSTAZIONE DI LAVORO: personal computer collegato alla rete comunale tramite il quale l'utente accede ai servizi;
- LOG: archivio delle attività di consultazione in rete;

MODALITÀ DI ACCESSO E DI UTILIZZO

Per accedere ai servizi informatici da una postazione di lavoro l'utente deve utilizzare un codice identificativo (id utente) e una parola chiave segreta (password).

Superato il sistema di autenticazione l'utente è collegato alla rete aziendale e ad internet senza ulteriori formalità.

Le postazioni di lavoro sono preventivamente individuate ed assegnate personalmente a ciascun utente; il collegamento alla rete da una postazione diversa da quella assegnata avviene solo in caso di esigenze di servizio preventivamente autorizzate dal datore di lavoro (ad es. utente assegnato a diverse sedi di lavoro, ...) e con l'utilizzo della coppia id utente – password personale.

L'utente, preso atto che la conoscenza della password da parte di terzi consente agli stessi l'accesso alla rete aziendale, l'utilizzo dei relativi servizi in nome dell'utente titolare e l'accesso ai dati cui il medesimo è abilitato, con possibilità di gestione degli stessi (ad es. visualizzazione di informazioni riservate, distruzione o modifica dei dati, lettura della propria posta elettronica, uso indebito di servizi ecc.), si impegna a:

- non cedere, una volta superata la fase di autenticazione, l'uso della propria stazione a personale non autorizzato, in particolar modo per quanto riguarda l'accesso a internet e ai servizi di posta elettronica;
- non lasciare incustodita ed accessibile la propria postazione una volta connesso al sistema con le proprie credenziali di autenticazione;
- conservare la password nella massima riservatezza e con la massima diligenza;
- non utilizzare credenziali (user-id e password) di altri utenti, nemmeno se fornite volontariamente o di cui si ha

casualmente conoscenza;

- mantenere la corretta configurazione del proprio computer non alterando le componenti hardware e software predisposte allo scopo né installando ulteriori software non autorizzati;
- non salvare file audio, video e file non istituzionali di qualsiasi tipo nelle connessioni di rete (ad esempio K: - S:) su cui viene eseguito giornalmente il back-up.

L'installazione di software o la modifica della configurazioni, la configurazione dei servizi di accesso ad internet e di posta elettronica viene eseguita esclusivamente da personale specializzato incaricato dal Comune.

Per prevenire la manomissione della configurazione hardware e software delle postazioni di lavoro, salvo rari casi necessari per il funzionamento di specifici applicativi, gli utenti sono configurati con diritti limitati.

Di qualsiasi azione o attività svolta utilizzando il codice identificativo e/o la password assegnata è responsabile l'utente assegnatario del codice.

L'utente è civilmente responsabile di qualsiasi danno arrecato al Comune e all'internet provider e/o a terzi in dipendenza della mancata osservazione di quanto previsto dal disciplinare.

L'utente può essere chiamato a rispondere civilmente, oltre che per i propri fatti illeciti, anche per quelli commessi da chiunque utilizzi il suo codice identificativo e/o password, con particolare riferimento all'immissione in rete di contenuti critici o idonei a offendere l'ordine pubblico o il buon costume così come definiti dalla giurisprudenza della corte di cassazione.

La violazione delle presenti disposizioni può comportare infine l'applicazione delle sanzioni disciplinari previste dal vigente Contratto Collettivo Provinciale di Lavoro, rimanendo ferma ogni ulteriore forma di responsabilità penale.

INTERNET

Tutti gli utenti cui è assegnata dal Comune una postazione di lavoro possono utilizzare internet, limitatamente ad una lista di siti istituzionali preventivamente individuati dal Comune (WHITE LIST) e previa identificazione con le modalità sopraillustrate (ID UTENTE/PASSWORD).

La lista dei siti (WHITE LIST) viene implementata nel tempo.

L'utilizzo ampio di internet, non limitato cioè alla lista di siti individuata come sopra, è autorizzato per ogni singolo utente dal Segretario comunale, previa richiesta adeguatamente motivata.

I responsabili delle strutture sono autorizzati automaticamente a tale tipo di accesso.

Al fine di prevenire il rischio di utilizzi impropri della rete, il Comune utilizza un sistema di filtri che impediscono l'accesso diretto a siti che non hanno natura istituzionale (BLACK LIST).

Oltre a tale sistema, è attiva una funzione di verifica del contenuto del sito; ove tale contenuto, secondo l'impostazione di una soglia predefinita, appaia non istituzionale viene visualizzato un messaggio che avverte l'utente; l'utente può quindi annullare la richiesta di accesso o accedere al sito, previa dichiarazione di responsabilità, rendendolo da quel momento disponibile a tutti gli utenti internet.

Le modalità di individuazione e di applicazione dei filtri sono decise dal Segretario comunale.

L'utente è direttamente responsabile dell'uso del servizio di accesso a internet, dei contenuti che vi ricerca, dei siti che contatta, delle informazioni che vi immette e delle modalità con cui opera.

Lo scarico di immagini, di file audio o musicali, di file video e in ogni caso di grandi quantità di dati in grado di degradare le prestazioni offerte dal servizio agli altri utenti può avvenire solo in casi eccezionali, su espressa autorizzazione del Segretario comunale, e in fasce orarie di basso utilizzo del canale internet (dalle ore 12.00 alle ore 14.30 e dopo le 17.00).

All'utente non è consentito:

- servirsi o dar modo ad altri di servirsi della stazione di accesso a internet per attività non istituzionali, per attività poste in essere in violazione del diritto d'autore o altri diritti tutelati dalla normativa vigente;
- utilizzare sistemi Peer to Peer (P2P), di file sharing, podcasting, webcasting o similari, così come connettersi a siti che trasmettono programmi in streaming (come radio o TV via WEB) senza previa autorizzazione del Segretario comunale;
- scaricare software dalla rete; eventuali necessità devono essere appositamente richieste al Segretario comunale;
- utilizzare internet provider diversi da quello ufficiale del Comune e la connessione di stazioni di lavoro aziendali alle reti di tali provider con sistemi di connessione diversi (es. modem) da quello centralizzato;
- usare la rete in modo difforme da quanto previsto dal presente documento e dalle leggi penali, civili e amministrative in materia di disciplina dell'attività e dei servizi svolti sulla rete.

POSTA ELETTRONICA

L'utilizzo del servizio di posta elettronica è consentito solo per ragioni di servizio agli utenti identificati con le modalità precedentemente illustrate, ai quali il Comune assegna una casella di posta personale e nominativa.

La casella del Servizio/Ufficio è accessibile solo in modalità di delega, previa richiesta e autorizzazione del Responsabile della struttura.

In caso di assenza dal servizio dell'utente per brevi periodi, è a disposizione apposita funzionalità di sistema che consente di inviare automaticamente un messaggio di risposta che avvisa il mittente dell'assenza del destinatario, individuando eventualmente altre modalità di contatto con la struttura.

In caso di assenza non programmata o dove non sia stata attivata la procedura di cui sopra, l'utente può delegare altro dipendente dell'ufficio a verificare il contenuto dei messaggi e ad inoltrare al Segretario comunale quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa.

All'utente non è consentito:

- utilizzare tecniche di "mail spamming" cioè di invio massiccio di comunicazioni a liste di distribuzione extraaziendali o di azioni equivalenti;
- utilizzare il servizio di posta elettronica per inoltrare catene di S. Antonio, appelli e petizioni (anche se possono sembrare veritieri e socialmente utili), giochi, scherzi, barzellette e altre e-mails che non siano di lavoro;
- allegare al testo delle comunicazioni materiale potenzialmente insicuro (ad es. programmi, scripts, macro), così come file di dimensioni eccessive.

L'utilizzo di liste di distribuzione riservate, comunemente riunite nella Rubrica Gruppi, che permettono l'invio di e-mails a una pluralità di utenti o a tutti gli utenti, è consentito solo a determinati soggetti, su autorizzazione del Segretario comunale; l'invio di messaggi con tali modalità è comunque limitato ai casi in cui il contenuto del messaggio sia effettivamente utile all'intero gruppo/i.

MONITORAGGIO E CONTROLLI

Il Comune può avvalersi di sistemi di controllo del corretto utilizzo degli strumenti di lavoro che consentono indirettamente un controllo a distanza dell'effettivo adempimento della prestazione lavorativa e determinano un trattamento di dati personali riferiti o riferibili al lavoratore nel rispetto di quanto previsto dal Provvedimento del garante della Privacy 1 marzo 2007 n. 13.

Le comunicazioni effettuate attraverso il servizio di posta elettronica interno sono riservate. Il contenuto di tali comunicazioni non può in nessun caso essere oggetto di alcuna forma di verifica, controllo o censura da parte del Comune, dell'internet provider o da parte di altri soggetti.

Le dichiarazioni di responsabilità effettuate dagli utenti internet per visualizzare e rendere da quel momento disponibile il sito/dominio sono a disposizione del Segretario comunale per le valutazioni di competenza.

Le attività sull'uso del servizio di accesso ad internet vengano automaticamente registrate in forma elettronica attraverso i LOG di sistema.

Il trattamento dei dati contenuti nei LOG può avvenire esclusivamente in forma anonima in modo tale da precludere l'identificazione degli utenti e/o delle loro attività.

I dati anonimi aggregati, riferibili all'intera struttura o a sue aree, sono a disposizione del Segretario comunale per le valutazioni di competenza e riguardano:

- per ciascun sito/dominio visitato le seguenti informazioni: il numero di utenti che lo visitano, il numero delle relative pagine richieste e della quantità di dati scaricati;
- per ciascun utente le seguenti informazioni: il numero di siti visitati, la quantità totale di dati scaricati, e le postazioni di lavoro utilizzate per la navigazione.

I dati personali contenuti nei log possono essere trattati in via eccezionale e tassativamente nelle seguenti ipotesi:

- per corrispondere ad eventuali richieste della polizia postale e/o dell'autorità giudiziaria;
- su richiesta del Segretario comunale quando si verifichi un evento dannoso o una situazione di pericolo che richieda un immediato intervento;
- su richiesta del Segretario comunale limitatamente al caso di utilizzo anomalo degli strumenti da parte degli utenti di una specifica struttura/area (rilevabile esclusivamente dai dati aggregati) e reiterato il mese successivo nonostante un necessario esplicito invito agli utenti da parte del Segretario comunale ad attenersi ai compiti assegnati ed alle istruzioni impartite.

I dati contenuti nei LOG sono conservati per il tempo strettamente necessario al perseguimento di finalità organizzative, produttive e di sicurezza, comunque non superiore a _____ mesi, e sono periodicamente cancellati automaticamente dal sistema.

I dati riguardanti il software installato sulle postazioni di lavoro (senza alcuna indicazione dell'utente che ha effettuato

l'installazione) possono essere trattati per finalità di verifica della sicurezza dei sistemi ed il controllo del rispetto delle licenze regolarmente acquistate.

INTERRUZIONE E CESSAZIONE D'UFFICIO DEL SERVIZIO

Eventuali interruzioni del servizio sono comunicate agli utenti.

Ai sensi della presente informativa, l'utilizzo del servizio di accesso ad internet cessa d'ufficio nei seguenti casi:

- se non sussiste più la condizione di dipendente o collaboratore autorizzato o non è confermata l'autorizzazione all'uso;
- se è accertato un uso non corretto del servizio da parte dell'utente o comunque un uso estraneo ai suoi compiti professionali;
- se vengono sospettate manomissioni e/o interventi sul hardware e/o sul software dell'utente impiegati per la connessione compiuti eventualmente da personale non autorizzato;
- in caso di diffusione o comunicazione imputabili direttamente o indirettamente all'utente, di password, procedure di connessione, indirizzo I.P. ed altre informazioni tecniche riservate;
- in caso di accesso doloso dell'utente a directory, a siti e/o file e/o servizi da chiunque resi disponibili non rientranti fra quelli per lui autorizzati e in ogni caso qualora l'attività dell'utente comporti danno, anche solo potenziale al sito contattato;
- in caso di concessione di accesso ad internet diretta o indiretta a qualsiasi titolo da parte dell'utente a terzi;
- in caso di violazione e/o inadempimento imputabile all'utente di quanto stabilito nei precedenti punti.
- in ogni altro caso in cui sussistono ragionevoli evidenze di una violazione degli obblighi dell'utente.