Allegato alla delib. n. 201
del 25/8/11

NORME DI COMPORTAMENTO PER L'ACCESSO ED UTILIZZO DEI SISTEMI INFORMATIVI, DELLE RISORSE INFORMATICHE, TELEMATICHE E TELEFONICHE DEL COMUNE DI TODI

IL SINDACO
(Avv. Antonino [illegible])

IL SEGRETARIO GENERALE
(Dott.ssa Paola [illegible])

INDICE

TITOLO V

USO DEL SERVIZIO DI RETE INTERNET

TITOLO VI

USO DEI SERVIZI DI RETE TELEFONICA FISSA E MOBILE

TITOLO VII

DISPOSIZIONI FINALI

PREMESSA

Negli ultimi anni le Risorse Informatiche, di Rete Telematica, di Rete Telefonica fissa e mobile che l'Amministrazione ha messo a disposizione dell'utenza per lo svolgimento della normale attività lavorativa, sono cresciute in misura considerevole in virtù di diversi fattori concomitanti con la riforma della Pubblica Amministrazione, quali ad esempio:

- *l'introduzione di nuovi software applicativi e gestionali;*
- *la capillare diffusione della posta elettronica per le comunicazioni interne ed esterne;*
- *l'utilizzo crescente di Internet quale abituale strumento di lavoro per la ricerca di informazioni e l'accesso a banche dati "on-line" in special modo ministeriali;*
- *l'ampio utilizzo della telefonia mobile e fissa per le comunicazioni di servizio.*

La diffusione dei citati strumenti e tecnologie ICT (Information & Communication Technology) ha incrementato di fatto la complessità gestionale dei Sistemi Informativi dell'Amministrazione, portando in primo piano numerosi problemi di carattere operativo e legislativo aventi importanti ripercussioni dal punto di vista delle responsabilità in capo al singolo utente finale e all'Ente.

Tra i problemi ricorrenti che attengono all'accesso ed all'utilizzo di sistemi e tecnologie ICT vi sono quelli legati alla sicurezza fisica e logica dei Sistemi Informativi automatizzati, quelli legati al trattamento delle informazioni da parte degli utenti, le problematiche legate alla proprietà intellettuale e diritto d'autore di banche dati e programmi informatici ed i temi specificatamente legati ai cosiddetti "computer crimes " (ovvero: crimini informatici), oltre alle eventuali , forme di abuso - nell'uso delle dotazioni aventi carattere istituzionale.

I fattori legati all'alta diffusione delle stazioni di lavoro informatizzate ad uso individuale oppure al sempre più esteso utilizzo della rete Internet hanno comportato, per i gestori dei sistemi e tecnologie ICT, la necessità di tenere alto il livello di attenzione nei confronti dei possibili comportamenti che il singolo addetto potrebbe attuare nel momento dell'accesso e dell'utilizzo delle risorse ad egli assegnate per lo svolgimento del lavoro d'ufficio.

Molti dei problemi sopra accennati, possono essere affrontati e risolti dalle Amministrazioni sensibilizzando e formando opportunamente l 'utenza sui temi afferenti il campo della cosiddetta "Informatica Giuridica ", laddove si specificano le norme di legge che devono essere rispettate al fine di un corretto utilizzo delle Risorse Informatiche, Telematiche e Telefoniche costituenti i Sistemi Informativi di un Ente o Azienda

Ai fini delle qui esposte Norme di comportamento, si è voluto però dare un 'accezione più ampia al termine "corretto" non limitandolo solo al concetto di utilizzo conforme alla normativa vigente, ma estendendolo alla necessità di perseguire, tramite adeguati comportamenti, un utilizzo efficiente ed efficace degli strumenti che l 'Amministrazione mette a disposizione dell'utenza, con il fine ultimo di raggiungere una gestione ottimale dei sistemi informativi automatizzati. In tale scenario si inserisce poi con forza la deliberazione n.13 del 1° marzo 2007 con la quale il Garante della Privacy ha dettato le linee guida che rendono obbligatoria la redazione di un disciplinare contenente le politiche interne atte a preservare sia la riservatezza dei dipendenti che la protezione dei dati aziendali, definendo inoltre i confini di liceità dell'attività di controllo del datore di lavor. A questo si è aggiunta la Direttiva N°02/09 del 26/05/2009 della Presidenza del Consiglio, Dipartimento della Funzione Pubblica avente ad oggetto "l'utilizzo di internet e della casella di posta elettronica istituzionale sul luogo di lavoro" .

Per esplicitare in maniera chiara i comportamenti ritenuti corretti o scorretti dall'Amministrazione Comunale, nella sua qualità di datore di lavoro, è stato preparato il presente testo "NORME DI COMPORTAMENTO PER L'ACCESSO ED UTILIZZO DEI SISTEMI INFORMATIVI, DELLE RISORSE INFORMATICHE, TELEMATICHE E TELEFONICHE" che disciplina le modalità di accesso e di utilizzo delle diverse risorse individuate nel seguito, richiamando i testi normativi vigenti, responsabilizzando l'utenza nei confronti di possibili comportamenti difformi dagli stessi, ma anche richiamando alcuni esempi pratici di errato utilizzo delle risorse a disposizione, secondo i dettami dell'Amministrazione di appartenenza.

Il testo è strutturato in capitoli distinti a seconda della tipologia di risorsa in esame, al fine di facilitare la lettura all'utente e consentire un rapido accesso all'argomento desiderato.

TITOLO I

PARTE GENERALE

Art. 1

Definizioni

• ***Amministrazione*** (denominato anche: Ente): il Comune di Todi, con sede in Piazza del Popolo n. 29/30-06059 Todi (PG).

• ***Codice della Amministrazione Digitale D.lgs. n. 82/2005*** (denominato anche: C.A.D.): Atto normativo che raccoglie la disciplina costituente il sistema legislativo sull'Amministrazione Digitale, aggiornato e integrato con il D.lgs. 30 dicembre 2010, n. 235 (nuovo CAD).

• ***D.lgs 30.06.2003 n°196*** (denominato anche "Codice"): Codice in materia di protezione dati personali.

• ***D.P.S.***: Documento Programmatico sulla Sicurezza dei dati e dei sistemi aggiornato almeno annualmente e deliberato dalla Giunta Comunale del Comune di Todi.

• ***Amministratore di sistema:*** è il personale del Servizio Informatico Comunale, Unità Operativa posta all'interno del Servizio personale e di supporto alla Direzione generale, (di qui in avanti SIC) o in rapporto contrattuale con l'Ente impiegato alla gestione e alla manutenzione degli impianti di elaborazione dati o di sue componenti. Ai fini del presente regolamento e nel rispetto del provvedimento del Garante per la Protezione dei dati personali del 27 novembre 2008, recepito nella Gazzetta Ufficiale. n. 300 del 24 dicembre 2008 tale figura ingloba anche gli amministratori di base dati, gli amministratori di apparati di rete e di sicurezza, gli apparati di sistemi software complessi. L'amministratore di sistema, dipendente del Comune di Todi viene nominato con Decreto del Sindaco, risulta quindi nel Documento Programmatico della Sicurezza.

• ***Account Operator:*** sono gli utenti abilitati, dall'Amministratore di Sistema, o da altro Ente esterno, ad amministrare l'accesso ai dati e le modalità di trattamento degli stessi per particolari procedure (es. banca dati anagrafe tributaria), in funzione del profilo di autorizzazione del servizio richiedente.

• ***Servizio Informatico Comunale (SIC):*** Unità Operativa posta all'interno del Servizio personale e di supporto alla Direzione generale di questo Comune, che è preposta all'acquisizione, alla gestione operativa e allo sviluppo delle tecnologie informatiche, telematiche e telefoniche dell'Amministrazione.

• ***Fornitore di assistenza sistemistica:*** sono i soggetti che operano per conto di Ditte, le quali per contratto di manutenzione, forniscono supporto sistemistico, sul software di sistema o sul software di base, all'Amministratore di Sistema o più in generale al SIC, vengono nominati dal competente Responsabile del Servizio personale su indicazione del SIC, che procede alla identificazione in maniera dettagliata delle attività svolte dalla Persona Fisica o Giuridica oltre alla lista relativa agli estremi identificativi delle persone fisiche preposte, quali "amministratori di sistemi complessi" (provvedimento del Garante per la Protezione dei dati personali del 27 novembre 2008, recepito nella Gazzetta Ufficiale. n. 300 del 24 dicembre 2008).

• ***Fornitore di assistenza su apparati di rete o di sicurezza di rete:*** sono i soggetti che operano per conto di Ditte che per contratto di manutenzione, forniscono supporto al sistema di networking comunale, sul software di sistema degli apparati attivi di rete sulla configurazione degli apparati di sicurezza della rete del SIC, vengono nominati dal Responsabile del Servizio personale su indicazione del SIC, che identifica in maniera dettagliata le attività svolte dalla Persona Fisica o Giuridica oltre alla lista relativa agli estremi identificativi delle persone fisiche preposte quali "amministratori di apparati di rete e di sicurezza" (provvedimento del Garante per la Protezione dei dati personali del 27 novembre 2008, recepito nella Gazzetta Ufficiale. n. 300 del 24 dicembre 2008).

• ***Fornitori di specifici applicativi e relativa assistenza:*** sono i soggetti che operano per conto di ditte che hanno fornito sistemi informativi e procedure informatiche in uso all'Ente e i quali per contratto forniscono assistenza e aggiornamenti. Vengono nominati dal Responsabile del Servizio personale su indicazione del SIC, che identifica in maniera dettagliata le attività svolte dalla Persona Fisica o Giuridica oltre alla lista relativa agli estremi identificativi delle persone fisiche preposte quali "amministratori di sistemi software complessi" (provvedimento del Garante per la Protezione dei dati personali del 27 novembre 2008, recepito nella Gazzetta Ufficiale. n. 300 del 24 dicembre 2008).

• ***Sistemi Informativi:*** sono tutte le banche dati ed i programmi informatici che costituiscono l'insieme delle risorse software acquisite o utilizzate su licenza da fornitori esterni o di proprietà dell'Amministrazione oppure disponibili tramite collegamenti interni o esterni all'Ente, installati su un qualunque sistema elaborativo server, client o di rete trasmissione dati su cui il SIC ha responsabilità di acquisizione, gestione operativa e sviluppo.

• ***Risorse Informatiche, Telematiche e Telefoniche:*** sono le attrezzature ed i dispositivi fisici come ad esempio:

I. le stazioni di lavoro, i personal computers (*asset*), i computer portatili, le stampanti ad uso individuale e per gruppi di lavoro (di rete);
2. le postazioni telefoniche fisse, gli apparati radiomobili cellulari, i centralini telefonici;
3. gli apparati di rete trasmissione dati e le altre attrezzature facenti parte della rete trasmissione dati comunale, della rete telefonica fissa e di quella mobile;
4. i collegamenti dati e telefonici acquisiti tramite noleggio da fornitori esterni oppure di proprietà dell'Amministrazione.

• ***Servizi di Rete Informatica, Telematica e Telefonica:*** sono i servizi disponibili tramite l'accesso alle Risorse Informatiche, Telematiche e Telefoniche dell'Amministrazione. Si intendono servizi di Rete Informatica quelli relativi all'autenticazione degli Utenti per l'utilizzo di stampanti di gruppo oppure per l'accesso e l'utilizzo del sistema di Posta Elettronica o di Internet. Esempi di servizi di Rete Telematica sono invece quelli che permettono il collegamento delle stazioni di lavoro ai sistemi dipartimentali anche da locazioni remote. Si intendono servizi di Rete Telefonica quelli resi disponibili attraverso l'impiego dei centralini telefonici (trasferimento di chiamata, deviazione ad altro numero, ecc) oppure dalla rete del gestore di rete telefonica mobile (segreteria telefonica, "dual-billing", ecc.).

• ***Utente:*** è la persona fisica, di norma identificabile nell'incaricato del trattamento dei dati ai sensi dell'art. 4, comma 1 (lettera h) e del responsabile del trattamento dei dati ai sensi dell'art. 4, comma 1, (lettera g) del Codice, che, previa abilitazione tecnica da parte del SIC, ha accesso ed utilizza i Sistemi Informativi e le Risorse Informatiche, Telematiche e Telefoniche dell'Amministrazione. Sono Utenti di norma:

- i dipendenti e i funzionari dell'Amministrazione;
- gli Amministratori dell'Ente;
- il personale esterno con incarichi professionali assegnati dall'Amministrazione;
- gli stagisti, i tirocinanti e gli addetti di società terze che prestano servizio o lavorano per conto dell'Amministrazione;

- i tecnici informatici dipendenti di società fornitrici dell'Amministrazione;
- tutti gli altri soggetti che, per periodi di tempo limitati o continuativi, hanno accesso e utilizzano i Sistemi Informativi e le Risorse Informatiche, Telematiche e Telefoniche dell'Amministrazione.

• ***File:*** è un agglomerato di dati disponibile per gli utenti del sistema.

• ***Log:*** è una raccolta di dati, automaticamente prodotti dal sistema, utili alla gestione dei sistemi di telefonia e derivati dall'impiego delle risorse informatiche e telefoniche.

• ***File di Log (o Log File):*** file nel quale vengono registrate le operazioni che l'utente compie durante la sua (sessione) attività, riferite alle risorse utilizzate e al loro impiego, all'accesso ai dati e/o alle banche dati di competenza dell'Ente.

• ***Backup:*** è la copia di riserva di un disco, di una parte del disco o di uno o più file o programmi su supporti di memorizzazione diversi da quello in uso. E' creata per scopi di archiviazione o per la salvaguardare file di valore da eventuali perdite qualora la copia originale venisse danneggiata o distrutta. E' anche detta copia di backup o file di backup.

• ***Sistema di Workflow*** *(impiegato anche per la funzionalità della intranet e del sistema di gestione delle determinazioni e deliberazioni e del protocollo):* promuove la gestione dei gruppi di lavoro collaborativi secondo il *workflow model*, o modello processuale . E' uno strumento *software* sviluppato per organizzare l'intermediazione dei flussi di informazione all'interno delle strutture produttive. Mediante l'utilizzo dei sistemi di *Workflow* l'Ente realizza i seguenti obbiettivi:

- Incremento dell'efficienza – l'automazione dei processi fornisce l'eliminazione dei passi non necessari;
- Migliore controllo del processo – mediante la standardizzazione dei metodi di lavoro e la disponibilità di strumenti di verifica;
- Flessibilità – il controllo del software sul processo di lavoro può essere programmato in base alle esigenze.

Art. 2

Oggetto e durata delle Norme

Con le presenti Norme vengono definite le modalità di accesso e di utilizzo dei Sistemi Informativi, delle Risorse Informatiche, Telematiche e Telefoniche ritenute corrette dall'Amministrazione. Compete difatti ai datori di lavoro assicurare la funzionalità dei citati sistemi, definendone le modalità d'uso nell'organizzazione dell'attività lavorativa, tenendo comunque in dovuto conto la disciplina in tema di diritti e relazioni sindacali.

La durata delle presenti Norme è a tempo indeterminato, fermo restando l'adeguamento delle stesse in dipendenza dei futuri cambiamenti della normativa di riferimento oppure di quelli dettati dall'evoluzione tecnologica che interesserà i sistemi e le tecnologie ICT.

Per quanto non espressamente specificato, le presenti Norme debbono essere interpretate secondo principi di correttezza e buona fede, oltre a rimandare, per il dettaglio di quanto inerente la sicurezza dei dati, al Documento Programmatico sulla Sicurezza già in uso presso l'Ente.

In caso di dubbi interpretativi o necessità di ulteriori informazioni circa i contenuti o l'applicazione delle presenti Norme e del D.P.S., gli Utenti sono invitati a rivolgersi immediatamente al SIC, inviando le proprie richieste o quesiti all'Amministratore di Sistema nominato con Decreto Sindacale.

Art. 3

Finalità delle Norme

L'adozione delle presenti Norme è finalizzata a garantire prioritariamente:

- l'onere in capo al datore di lavoro di indicare chiaramente ed in modo particolareggiato quali siano le modalità di utilizzo degli strumenti messi a disposizione ritenute corrette e in che misura e con quali modalità vengano effettuati controlli;
- il rispetto delle leggi in materia di trattamento delle informazioni e dei dati trattati dagli utenti dei sistemi informativi, anche tenuto conto delle esigenze di tutela della privacy e della sicurezza del trattamento degli archivi informatici;
- il rispetto delle leggi in materia di tutela giuridica dei programmi per elaboratore e delle banche dati;
- il rispetto delle leggi in materia di crimini informatici.

Inoltre le presenti Norme mirano ad assicurare:

- la riservatezza delle informazioni trattate con i Sistemi Informativi dell'Amministrazione e la sicurezza nello scambio di informazioni da parte degli Utenti;
- il corretto utilizzo delle Risorse Informatiche, Telematiche e Telefoniche da parte degli Utenti per lo svolgimento del lavoro d'ufficio al fine di garantire la massima efficienza nell'utilizzo delle Risorse stesse ed evitare ogni forma di abuso;
- la massima disponibilità e continuità di servizio dei Sistemi Informativi dell'Amministrazione, evitando quindi possibili interruzioni o ritardi, nell'interesse degli Utenti e della collettività.

Art. 4

Conservazione delle informazioni

Si evidenzia che, oltre i tabulati inerenti i dati del traffico telefonico o della navigazione Internet, depositati presso i provider del servizio Internet di telefonia fissa e mobile, richiedibili al gestore, sussistono all'interno dei sistemi informativi dell'Ente una variegata e notevole quantità di *file di log* che vengono memorizzati in forma centralizzata o localizzata a fini manutentivi e diagnostici per un tempo variabile da caso a caso, in base alle diverse configurazioni che il personale deputato all'Amministrazione degli stessi ritiene opportuno e necessario nel rispetto del principio di correttezza e trasparenza. A ciò si aggiunge una strategica ed articolata strategia di *backup* anch'essa centralizzata che comporta l'archiviazione a scopi di ripristino praticamente di tutti i dati salvati negli archivi del software di base per il funzionamento delle procedure informatiche o nelle apposite directory o base dati messe a disposizione degli uffici e dei servizi opportunamente configurate per consentire l'accesso soltanto agli utenti abilitati secondo le indicazioni dei rispettivi responsabili del trattamento. Tale capillare lavoro di archiviazione avviene al fine di assicurare la continuità e la funzionalità di un servizio pubblico essenziale quale quello del Comune di Todi. L'unico soggetto autorizzato ad accedere a tali informazioni, per soli scopi manutentivi e diagnostici, è il personale tecnico del SIC ed il personale facente parte delle ditte fornitrici di servizi di assistenza sistemistica o applicativa preventivamente identificato. Risulta quindi escluso qualsiasi altro accesso lecito a tali informazioni da parte di qualsivoglia soggetto (Sindaco, Amministratore, Segretario Generale, Direttore Generale, Capo Servizio, Commissario Straordinario ecc.) senza una esplicita e motivata richiesta formale da inoltrarsi al SIC, tesa ad evitare qualsiasi forma di illecito controllo a distanza dei lavoratori. Analisi a parte meritano i *file di log* inerenti i dati personali relativi agli accessi ad Internet e al traffico telematico, quali ad esempio quelli registrati dal *proxy server* (computer che funge da intermediario nella comunicazione attraverso la rete internet con l'esterno), per i quali, sebbene si

effettui "una cancellazione periodica ed automatica" nonché "un trattamento dati in forma anonima o tale da precludere l'immediata identificazione degli utenti mediante opportune aggregazioni" è fissato in quarantotto ore il tempo massimo di archiviazione dei *log file* contenenti anche il dettaglio delle attività di navigazione svolte dal singolo utente, ove per dettaglio si intende sia l'URL che il particolare della pagina visitata e ciò al fine di garantire le previste attività di controllo tecnico, economico e statistico del servizio. In aggiunta a quanto esposto si evidenzia che l'introduzione di *software* di produttività basato su sistemi di *Workflow* (Art.1) per sua natura sottende l'automazione del processo e la condivisione dell'informazione anche attraverso la gestione della comunicazione e il passaggio di compiti da un collaboratore all'altro. Pertanto un sistema di *Workflow* fissa e registra le attività svolte dall'utente all'interno di esso indicando i metodi esecutivi (esempio di azione: modifica) e quelli temporali (data e ora) utili alla produzione di un determinato atto/documento, ciò anche per i c.d. processi intermedi. La conservazione di queste informazioni è legato al ciclo di vita del software di *Workflow* in quanto sono parte integrante e sostanziale del sistema stesso e quindi del patrimonio informativo del Comune di Todi. I tempi di conservazione dei *log file* relativi all'accesso al dominio (*log on* al sistema di rete del Comune di Todi) è fissato in sei mesi. I tempi di conservazione dei log file relativi all'utilizzo delle periferiche rimovibili (dispositivi di archiviazione di massa esterni, chiavette USB, CDRW e DVDRW) variano in funzione delle risorse informatiche sottoposte a controllo.

Art. 5

Effettuazione Controlli

L'Amministrazione Comunale, nella sua qualità di datore di lavoro, si riserva di effettuare controlli in conformità alla legge, tesi alla verifica dell'effettivo adempimento della prestazione lavorativa e, se necessario, al corretto utilizzo degli strumenti di lavoro (artt. 2086, 2087 e 2104 Codice Civile). Nell'esercizio di tale prerogativa l'Amministrazione rispetterà la libertà e la dignità dei lavoratori, attenendosi a quanto riportato nello Statuto dei Lavoratori, fornirà informazione preventiva (quale quella formulata mediante pubblicizzazione delle presenti norme, anche attraverso l'inserimento nell'area comune della intranet riferita alla Privacy), si avvarrà di appositi soggetti preposti e rispetterà i principi di pertinenza e non eccedenza e ogni quant'altro riportato nel disposto di cui alla determinazione del Garante della privacy n. 13 del 1.03 2007 e nella Direttiva N°02/09 del 26/05/2009 della Presidenza del Consiglio, Dipartimento della Funzione Pubblica avente ad oggetto "l'utilizzo di internet e della casella di posta elettronica istituzionale sul luogo di lavoro", nel rispetto delle quali verranno avviate le occasionali o mirate attività di controllo. Tali attività di controllo, per quanto possibile, verranno effettuate secondo principi di gradualità, quindi in forma preliminare su dati aggregati e sempre secondo principi di pertinenza e non eccedenza. Il controllo anonimo può concludersi con un avviso generalizzato relativo ad un utilizzo anomalo degli strumenti aziendali e con l'invito ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite. In caso di riscontro di abusi singoli o reiterati, verranno inoltrati appositi preventivi avvisi collettivi o individuali ed effettuati controlli nominativi o su singoli dispositivi, account o postazioni di lavoro. Il SIC, nell'interesse dell'Amministrazione, utilizzando i sistemi informativi, per esigenze proprie organizzative, ovvero per rilevare anomalie e/o per manutenzioni, si avvale legittimamente, nel rispetto sempre dello Statuto dei lavoratori (art. 4, comma 2), di sistemi che consentono indirettamente un controllo a distanza (c.d. controllo preterintenzionale) e determinano un trattamento lecito di dati personali riferiti o riferibili ai lavoratori.

Con le stesse modalità e con le stesse prerogative il SIC effettua inoltre d'ufficio una serie di controlli saltuari ed occasionali tesi a verificare la funzionalità e la sicurezza del sistema.
Al fine di rispettare le procedure di informazione e di consultazione dei lavoratori e dei sindacati in relazione all'introduzione o alla modifica di sistemi automatizzati per la raccolta e l'utilizzazione dei dati, nonché alla introduzione o modificazione di procedimenti tecnici destinati a controllare i movimenti o la produttività dei lavoratori, si evidenzia come il precedente art.4 "Conservazione delle informazioni" debba intendersi risolutivo in tal senso.

Art. 6

Soggetti preposti al monitoraggio

Soggetto preposto dall'Amministrazione al monitoraggio di cui all'art. 5 risulta essere il SIC, oltre ai diversi Amministratori per le loro specifiche aree di competenza nel rispetto di quanto sancito all'Art.4 dal Provvedimento del Garante del 27 novembre 2008 (G.U. n.300 del 24 dicembre 2008) recante le "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" Art.2 lett.e), indica la necessità di istituire dei controlli sull'operato degli amministratori di sistema con cadenza almeno annuale. Tale attività è svolta dal Titolare del Trattamento (o da un suo addetto) ed è volta a verificare la rispondenza delle misure organizzative, tecniche e di sicurezza poste in essere nel sistema, riguardanti i trattamenti dei dati personali previsti rispetto alle norme vigenti.

Art. 7

Conseguenze abusi

Qualora si constati che i Sistemi informativi, le risorse informatiche, telematiche o telefoniche siano state indebitamente utilizzate, fatte salve ulteriori conseguenze di natura penale, civile e amministrativa, l'Amministrazione procederà disciplinarmente nei confronti dei soggetti che hanno compiuto abusi, ai sensi del Codice disciplinare e del CCNL vigente.

Art. 8

Compiti del Servizio Informatico Comunale

Il Servizio Informatico Comunale (come definito al precedente art.1) si assume l'onere di:

- adottare tutti i dispositivi di sicurezza necessari per proteggere l'integrità fisica e logica dei sistemi ed apparecchiature informatiche, telematiche e telefoniche che ha in gestione;
- implementare opportuni meccanismi di controllo e monitoraggio, anche a livello preventivo, atti ad evitare possibili intrusioni ai Sistemi Informativi ed alle apparecchiature informatiche, telematiche e telefoniche ed abusi nell'utilizzo delle stesse, essendo individuato quale soggetto preposto alle attività di monitoraggio;
- responsabilizzare e formare (nel caso specifico della formazione compatibilmente con le disponibilità di bilancio) gli Utenti circa le conseguenze penali, civili ed amministrative connesse all'uso indebito o improprio degli strumenti informatici, telematici e telefonici.

Per raggiungere gli obiettivi sopra descritti il SIC provvede al continuo aggiornamento dei piani per la sicurezza informatica dell'Amministrazione, anche mediante redazione di specifici atti, adottando le più recenti tecnologie disponibili sul mercato ICT, al fine di implementare misure idonee a salvaguardia delle Risorse Informatiche, Telematiche e Telefoniche dell'Ente. Al SIC vengono inoltrate le richieste di installazioni, realizzazioni e ristrutturazioni hardware e software che devono essere valutate congiuntamente con il Responsabile del Servizio interessato. Al SIC spetta la verifica tecnica della compatibilità degli strumenti richiesti con l'infrastruttura di rete e la normativa vigente, con particolare riferimento alla sicurezza delle banche dati dell'Ente. In particolare, non possono essere effettuate realizzazioni, ristrutturazioni, acquisizioni e installazioni

di attrezzature e/o componenti hardware e/o software senza preventiva valutazione e visto tecnico del Responsabile SIC. Nel caso in cui gli strumenti proposti non possano, per ragioni tecniche, essere installati, saranno individuate, ove possibile e nei limiti della tecnologia, soluzioni alternative, tecnicamente fattibili, d'intesa tra il SIC e il servizio interessato. Gli strumenti e i sistemi hardware/software tecnicamente utilizzabili saranno resi disponibili dal SIC (o da personale tecnico da questi esplicitamente autorizzato), compatibilmente con le licenze d'uso disponibili e le risorse economiche. Le licenze d'uso devono essere conservate presso il SIC, così da consentire le operazioni di verifica della disponibilità e l'eventuale installazione.

Al SIC e ai fornitori di assistenza (di sistema, hardware e software) viene riservata la facoltà di accedere in un qualunque momento alle Risorse Informatiche, Telematiche e Telefoniche, ai soli fini dell'espletamento di compiti manutentivi e di monitoraggio sulle Risorse stesse e sui Sistemi, ai fini della salvaguardia della sicurezza e della corretta funzionalità dei Sistemi Informativi dell'Amministrazione, nel rispetto della riservatezza dei dati personali di cui al D.Lgs. 30 giugno 2003, n. 196. Tale attività tecnica, funzionale ai compiti istituzionali, essendo atta e necessaria a garantire la corretta efficienza dei sistemi informativi, oltre a raffigurarsi come "determinata, esplicita e legittima" ed essere svolta dai soli soggetti "Preposti" (SIC) verrà svolta comunque "nella misura meno invasiva possibile" e secondo principi di "Pertinenza e non eccedenza". Resta fermo l'obbligo, per i soggetti facenti parte del SIC preposti al succitato trattamento dati di svolgere solo operazioni strettamente necessarie al perseguimento delle relative finalità, senza realizzare attività di controllo a distanza, anche di propria iniziativa. L'eventuale richiesta di accesso ad informazioni attinenti i lavoratori che si configurino come "attività di controllo" debbono essere inoltrate al SIC dall'Amministrazione, tramite di richiesta scritta formalizzata dal Segretario Generale o altro soggetto appositamente autorizzato, nel rispetto dei succitati principi ed in particolar modo del disposto di cui alla predetta determinazione del Garante della Privacy n.13 del 01.03.2007. Anche in conseguenza delle predette regole di condotta dei soggetti che operano quali amministratori di sistema o similari in capo al SIC, resta ferma la necessità che sia svolta da questi ultimi apposita attività formativa sui profili tecnico-gestionali e di sicurezza delle reti, sui principi di protezione dei dati personali e sul segreto nelle comunicazioni (vedi regola 19.6 allegato B, D.Lgs. 196/2003, Parere 8/2001 Garante, DPS dell'Ente) e strumentali dell'Ente.

TITOLO II

USO DELLE RISORSE INFORMATICHE

Art. 9

Generalità

Le Risorse Informatiche che vengono assegnate agli Utenti costituiscono uno strumento di lavoro. L'insieme delle Risorse Informatiche a disposizione degli Utenti è suddiviso di norma in due categorie:

* Risorse assegnabili individualmente, cioè per via nominativa, al singolo Utente;
* Risorse non assegnabili individualmente al singolo Utente, in quanto condivise nell'accesso e nell'utilizzo tra più Utenti.

Per Risorsa Informatica assegnabile nominalmente all'Utente, si intende ad esempio:

- la stazione di lavoro (denominata anche: personal computer o PC), costituita di solito dall'unità base elaborativa dotata di supporti di memoria fissi e rimovibili, video, tastiera e mouse;
- la stampante eventualmente collegata alla stazione di lavoro di cui sopra (condivisa o meno con altri utenti);
- supporti di firma digitale;
- gli eventuali altri dispositivi accessori direttamente collegati alla stazione di lavoro (es. scanner, etichettatrici, ecc).

Per Risorsa Informatica non assegnabile nominalmente all'Utente, ma a disposizione di gruppi di Utenti definiti dal SIC, si intende ad esempio:

- una stampante di gruppo o di rete collegata alla rete trasmissione dati comunale utilizzata da più Utenti;
- uno spazio di memorizzazione su un sistema elaborativo dipartimentale (DB server, file server, intranet, NAS, ecc.) utilizzato da più Utenti che accedono e condividono le informazioni ivi contenute.

L'Utente è reso edotto che qualunque utilizzo delle Risorse Informatiche o comportamento da parte dell'Utente non strettamente inerente l'attività lavorativa può dare luogo a malfunzionamenti o disservizi sia nei confronti dell'utenza interna sia di soggetti e persone esterne, causando maggiori costi per l'Amministrazione e diseconomie nella gestione dei sistemi e delle attrezzature informatiche. Taluni utilizzi impropri delle Risorse Informatiche possono inoltre mettere a rischio la sicurezza informatica dei Sistemi Informativi dell'Amministrazione.

Art. 10

Accesso

L'accesso alle Risorse Informatiche è riservato ai soli Utenti, previa assegnazione delle stesse e delle credenziali da parte del SIC. L'assegnazione di Risorse Informatiche ad un Utente avviene di norma dietro presentazione al SIC di una richiesta del responsabile del servizio da cui l'Utente dipende, oppure su iniziativa del SIC nel caso di Risorse che rientrano in piani di sostituzione tecnologica di sistemi ed apparecchiature informatiche ormai obsolete. Il piano di sostituzione delle risorse informatiche è stabilito nel "Piano di razionalizzazione delle dotazioni strumentali" approvato dalla Giunta Comunale. Ogni Risorsa Informatica viene assegnata nominalmente a un Utente o, qualora si tratti di risorsa condivisa non assegnabile individualmente bensì ad un gruppo di Utenti, al Responsabile di Servizio o suo delegato dal quale l'Utente dipende. Il SIC, ricevuta la richiesta di assegnazione della Risorsa, provvede all'assegnazione fisica della stessa sul posto di lavoro dell'Utente individuato, comunicando la relativa accoglibilità o meno, previa verifica di congruità tecnica ed organizzativa, tenendo conto di fattori quali:

- disponibilità di Risorse Informatiche a magazzino;

- piani periodici di acquisizione di nuove attrezzature informatiche;
- carichi di lavoro connessi alle attività tecnico-amministrative degli uffici del SIC.

La comunicazione succitata indica altresì, in caso di riscontrata accoglibilità, i tempi previsti di evasione della richiesta medesima.
Tutte le richieste di assegnazione di Risorse Informatiche pervenute al SIC vengono evase nel più breve tempo possibile, di norma nel rispetto dell'ordine di arrivo delle stesse e tenendo in debito conto le situazioni organizzative e le esigenze debitamente segnalate che impongono particolare urgenza. Ciascun Utente assegnatario di una Risorsa Informatica sottoscrive la dichiarazione di presa in carico e di accettazione delle norme contenute nel presente regolamento.

Articolo 11

Utilizzo

Non è consentito all'Utente la modifica delle caratteristiche fisiche impostate sulla Risorsa Informatica assegnata ad uso individuale né sulla Risorsa condivisa con altri Utenti. In particolare, nel caso di stazione di lavoro, non è consentito all'Utente di provvedere:
- all'installazione o alla rimozione di qualunque dispositivo interno o esterno (in particolare dispositivi di comunicazione quali: modem, telefoni cellulari, dispositivi UMTS, chiavette internet ecc.) all'unità base elaborativa o ad altre unità ad essa collegate al fine di modificare le caratteristiche tecniche o di funzionamento della stessa;
- alla modifica di qualsiasi parametro di configurazione o di funzionamento relativo a caratteristiche tecniche dell'unità base elaborativa.

È espressamente vietato all'Utente provvedere in via autonoma allo spostamento fisico di una Risorsa Informatica, ovvero di parti e componenti della stessa, nell'ambito dello stesso ufficio, tra diversi uffici o tra le sedi dell'Amministrazione, senza l'autorizzazione del SIC e del personale tecnico incaricato dal SIC per la riconfigurazione logica e di rete.
E altresì severamente vietato all'Utente, in particolar modo se dipendente di società esterne, il collegamento, anche temporaneo, alla rete di trasmissione dati comunale, di sistemi ed apparecchiature informatiche di proprietà personale o aziendale, salvo la preventiva autorizzazione e supervisione da parte del SIC.
E' responsabilità dell'Utente provvedere affinché la stazione di lavoro assegnata ad uso individuale venga spenta ogni giorno prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio.
L'Utente è consapevole che lasciare un elaboratore incustodito può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. Per questo motivo viene suggerito all'Utente di disattivare mediante logout la stazione di lavoro ad uso individuale. Il SIC ha provveduto ad implementare una regola nel sistema che abilita lo screen saver automaticamente dopo dieci minuti di inattività della postazione. Non è consentita l'attivazione della password di accensione (altresì denominata "password di BIOS o di SETUP") o di altre password e/o di altro blocco fisico o logico su una Risorsa Informatica ne tantomeno crittografare dati aziendali senza la preventiva autorizzazione da parte del SIC. Ogni Utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il SIC nel caso in cui vengano rilevati dall'apposito software antivirus virus informatici sulla stazione di lavoro ad egli assegnata o nei casi di dubbia provenienza dei supporti. Al fine di tutelare le proprie banche dati, l'Ente ha implementato dei servizi di protezione dell'asset (computer) atti a inibire automaticamente l'utilizzo di supporti esterni di memorizzazione per la copia di file su chiavi USB, o hard disk esterni da disco fisso o da rete. Nel caso straordinario di utilizzo dei supporti rimovibili per il trattamento delle informazioni (es. floppy disk, CDRW, DVD-RW, chiavette USB ecc.) questi possono essere reimpiegati solamente quando le informazioni precedentemente contenute siano state cancellate in maniera definitiva; in caso contrario è responsabilità dell'Utente provvedere affinché gli stessi supporti vengano distrutti. Gli utenti vengono forniti soltanto di chiavi USB con sezione cifrata protetta da password. Le password delle chiavi USB assegnate nominalmente dal SIC devono essere comunicate all'Amministratore di Sistema. L'Utente è responsabilizzato sul fatto che, nel caso di restituzione in via definitiva di una stazione di lavoro, è suo preciso

compito avvertire preventivamente il SIC della eventuale presenza di archivi informatici contenenti dati memorizzati nella stessa, onde evitare la perdita di dati a fronte del ricondizionamento della stazione di lavoro.

Art. 12

Assistenza Tecnica

Tutti gli interventi di assistenza tecnica prestati da parte dei tecnici informatici appartenenti al SIC o da parte di soggetti terzi debitamente autorizzati (Help-desk), attuati per la risoluzione di malfunzionamenti su Risorse Informatiche, possono essere eseguiti solamente con il consenso esplicito (anche verbale) dell'Utente o con l'assenso del Responsabile di Servizio o suo delegato da cui egli dipende. Qualora ciò non fosse possibile, il SIC non si assume alcuna responsabilità per la mancata effettuazione dell'intervento stesso ed in particolare per ogni ritardo nelle attività lavorative dell'Utente derivato dal mancato intervento.
L'apertura di chiamata mediante richiesta formale al SIC anche tramite e-mail all'indirizzo del SIC ha valore autorizzativo in tal senso, salvo che per interventi tecnici di carattere generale decisi dal SIC (es.: aggiornamenti e riconfigurazioni), che non necessitano di autorizzazione preventiva.
In particolare il tecnico informatico potrà accedere alle Risorse Informatiche assegnate all'Utente per fornire ausilio nella soluzione dei problemi tecnici da egli segnalati, anche remotamente mediante tecniche di telediagnosi (ad esempio visualizzando il contenuto dello schermo video della stazione di lavoro o il contenuto degli archivi), solamente se autorizzato come sopra precisato.
Al termine di ciascun intervento di assistenza tecnica, se richiesto, il tecnico informatico rilascerà apposita comunicazione scritta (anche via e-mail) attestante l'intervento eseguito che l'Utente dovrà firmare per accettazione.

Art. 13

Stazioni di lavoro portatili

L'Utente, qualora risulti assegnatario di una stazione di lavoro portatile (PC portatile o Notebook), è responsabile della custodia della stessa sia durante gli spostamenti che durante l'utilizzo nel luogo di lavoro. I PC portatili utilizzati anche per attività esterne all'Amministrazione (es. convegni, visite in azienda), in caso di allontanamento, devono essere custoditi in un luogo protetto. Alle stazioni di lavoro portatili si applicano le stesse regole di utilizzo previste per le stazioni di lavoro connesse di norma alla rete di trasmissione dati comunale. Considerata la oggettiva vulnerabilità del computer portatile, all'utente a cui è assegnato l'elaboratore è fatto espresso divieto di conservare archivi contenenti dati "personali" all'interno di esso. Qualora per motivi di servizio l'assegnatario di un computer portatile necessiti di attività di consultazione delle banche dati esistenti nell'Ente, il SIT dietro motivata richiesta, provvederà ad abilitare opportuni collegamenti in modalità Rete Virtuale Privata (VPN) atti a consentire tale accesso da sede remota.

Art. 14

Protezione Antivirus

Tutte le stazioni di lavoro assegnate agli Utenti sono protette contro il rischio di attacco al sistema informatico a opera di virus o altro software aggressivo di cui all'art. 615 quinquies del codice penale; la protezione si estende anche ai sistemi dipartimentali (server) che ospitano informazioni e programmi utilizzati dagli Utenti ed al sistema di Posta Elettronica.
La protezione avviene mediante l'utilizzo di idonei programmi installati sui sistemi la cui efficacia e aggiornamento sono verificati dal SIC conformemente a quanto disposto dall'Allegato B del D.Lgs. 30 giugno 2003 n. 196; tuttavia l'Utente è tenuto ad assumere comportamenti tali da ridurre al minimo tale

rischio. Non è consentito l'utilizzo di supporti di memorizzazione come floppy disk CD-ROM nastri magnetici ecc. di provenienza dubbia o ignota oppure di proprietà dell'Utente. In ogni caso qualunque dispositivo di memorizzazione di provenienza esterna all'Ente dovrà essere prudenzialmente verificato da parte dell'Utente mediante il programma antivirus prima del suo utilizzo. Nel caso vi sia il sospetto della presenza di un virus informatico su un supporto di memorizzazione, quest'ultimo dovrà essere consegnato tempestivamente al SIC per la successiva analisi e trattamento. Nel caso in cui venga effettivamente rilevata dall'Utente la presenza di un virus su una stazione di lavoro dal programma software antivirus ivi installato, questi dovrà immediatamente: sospendere ogni elaborazione in corso senza spegnere la stazione di lavoro e segnalare tempestivamente l'accaduto al SIC.

USO DEI SISTEMI INFORMATIVI

Art. 15

Generalità

I Sistemi Informativi utilizzati dagli Utenti costituiscono uno strumento di lavoro. L'utilizzo dei Sistemi Informativi da parte degli Utenti è preceduto di norma dal preventivo rilascio da parte del SIC di una specifica autorizzazione per l'accesso alle risorse informative (o banche dati) che compongono quel determinato sistema, e nell'autorizzazione all'utilizzo dei programmi informatici che permettono il trattamento delle informazioni e dei dati ivi contenuti. Costituiscono esempi di risorse informative:

a) le banche dati accessibili tramite collegamenti ai sistemi gestionali dell'Amministrazione, di norma memorizzate in elaboratori dipartimentali (server) gestiti dal SIC, come ad esempio il sistema di contabilità, del personale, dell'anagrafe comunale, di protocollo, della gestione degli atti dirigenziali ecc.;

b) le banche dati accessibili tramite collegamenti dedicati ai servizi di rete informatica gestiti da soggetti esterni (es. ANCI, Ministero dell'Economia, Motorizzazione Civile, Leggi d'Italia, ecc), anche via Internet;

c) le banche dati memorizzate nella stazione di lavoro dell'Utente finale o su spazi di memorizzazione su server dipartimentali, anche condivisi, gestite da programmi informatici regolarmente autorizzati dal SIC.

Costituiscono invece esempi di programmi informatici che permettono il trattamento delle informazioni contenute nelle banche dati sopra descritte:

a) programmi emulatori di terminali video come Windows Terminal Server, ecc.;

b) programmi di produttività individuale come MSOffice, Open Office, ecc.;

c) altri programmi client specializzati o sviluppati ad hoc dai fornitori per usi particolari come AutoCAD/AutoCAD Map, Acrobat Reader, ecc.

L'Utente che accede ai Sistemi Informativi è responsabilizzato sul fatto che tutti i dati personali oggetto di trattamento contenuti negli archivi informatici degli stessi sono protetti ai sensi del D.Lgs. 30 giugno 2003. n. 196, e a tale scopo oltre che per garantire la continuità e la funzionalità del servizio istituzionale dell'Ente è fatto obbligo a tutti gli utenti di memorizzare i dati inerenti l'attività lavorativa nelle apposite "cartelle individuali e/o di gruppo di rete" risiedenti nei file server e nel DB server dell'Ente, consultabili anche attraverso la intranet. Tale organizzazione del lavoro consente all'Amministrazione di garantire la completa e continua disponibilità dei dati mediante effettuazione di backup pianificati come indicato nel DPS, ad opera del SIC. Pertanto in caso di guasto, malfunzionamento o sostituzione di una postazione di lavoro informatizzata, nonché di cancellazioni o modifiche accidentali, potranno essere recuperati soltanto i documenti preventivamente salvati tramite questo servizio, mentre qualsiasi documento non preventivamente salvato in quest'area, non potrà in alcun caso essere recuperato, con possibile danno per l'Ente. Gli utenti sono quindi edotti che tutti i dati memorizzati sulla NAS o sui server interni dell'Ente sono archiviati in forma precisa e puntuale (ivi comprese le immagini macchina di alcuni PC dedicati a particolari funzioni) per le motivazioni e con le modalità di cui al precedente art. 4 e che eventuali forme di controllo sul rispetto del corretto uso degli strumenti di lavoro e dell'effettivo adempimento della prestazione lavorativa avverranno esclusivamente secondo quanto indicato al precedente art. 5 ed ai sensi della deliberazione del Garante della Privacy n.13 del 01.03.2007. Essendo stato appositamente e chiaramente specificato l'uso istituzionale e non personale dei sistemi di memorizzazione dei dati assegnati dall'ente agli utenti, resta quindi esclusa qualsiasi aspettativa di confidenzialità da parte degli utilizzatori di tali sistemi lavorativi. In relazione all'utilizzo del servizio intranet o delle cartelle condivise, l'utente nell'utilizzo delle risorse assegnate è tenuto a:

a) Memorizzare, ove non sia diversamente ed automaticamente disposto da parte dello specifico

software utilizzato, i documenti inerenti alla propria attività esclusivamente nelle quote di spazio disco accessibile o condivisibile in rete denominato:

a. Cartella personale "home" utente;
b. Cartella del servizio personale (riferita ai soli componenti della U.O. di appartenenza);
c. Cartella del servizio pubblica (riferita a tutti gli appartenenti al dominio dell'Ente).

b) Aggiornare i documenti archiviati sia eliminando quelli non più necessari (facendo particolare attenzione ai file resi disponibili nelle cartelle pubbliche per soli fini di scambio e tenuto conto che sono accessibili a tutti) sia chiedendone la masterizzazione al SIC su supporti rimovibili, nel caso in cui debbano essere conservati per sicurezza;
c) Prestare attenzione alla duplicazione dei dati in modo da evitare un'archiviazione ridondante e un conseguente spreco di risorsa si disco.

L'Utente è consapevole che le banche dati sono tutelate dalla normativa sul diritto d'autore di cui alla legge 22 aprile 1941, n. 633 *("Protezione del diritto d'autore e di altri diritti connessi al suo esercizio")* e dal relativo Regolamento di esecuzione approvato con R.D. 18 maggio 1942, n. 1369 e successive modificazioni, nonché dal D.Lgs. 29 dicembre 1992, n. 518 *("Attuazione della direttiva 9112501CE relativa alla tutela giuridica dei programmi per* elaboratore") e dalla legge 18 agosto 2000, n. 248 *("Nuove norme di tutela del diritto d'autore"),* e pertanto si impegna a non divulgarne i contenuti informativi al di fuori di motivi di servizio.

Sono altresì vietate ai sensi del D.Lgs. 6 maggio 1999, n. 169 *("Attuazione della direttiva 96/9/CE relativa alla tutela giuridica delle banche di dati"),* la riproduzione, la distribuzione, la comunicazione, totale o parziale, con qualsiasi mezzo e in qualsiasi forma delle banche dati che per la scelta o la disposizione del materiale costituiscono una creazione intellettuale dell'autore.

L'Utente è altresì responsabilizzato sul fatto che taluni comportamenti impropri attuati nell'accesso e nell'utilizzo dei Sistemi Informativi possono violare le norme in tema di criminalità informatica di cui alla legge 23 dicembre 1993, n. 547. *("Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tura di criminalità informatica")*

Art. 16

Accesso

L'accesso ai Sistemi Informativi è riservato ai soli Utenti previo rilascio di opportuna abilitazione all'uso da parte del SIC o di un Amministratore nominato per una particolare area funzionale (sistemistica, applicativa ecc.). La concessione dell'abilitazione all'accesso di una specifica risorsa informativa o di utilizzo di programma informatico da parte di un Utente avviene dietro presentazione, a chi è deputato a fornire le credenziali di accesso, di una richiesta motivata da parte del Responsabile di Servizio o suo delegato da cui l'Utente finale dipende.

Nella richiesta viene specificata la risorsa informativa ovvero il programma informatico per il quale viene chiesto l'accesso e il livello di utilizzo da parte dell'Utente, viene inoltre indicata una specifica assunzione di responsabilità in merito ad una tempestiva comunicazione, stesso mezzo, dell'eventualità di perdita delle prerogative di accesso da parte dello stesso soggetto richiedente. Ogni abilitazione all'accesso di un sistema informativo viene assegnata esclusivamente per via nominale all'Utente finale.

Chi è deputato a fornire le credenziali di accesso, ricevuta la richiesta di accesso alla risorsa informativa, provvede alle operazioni tecniche che permettono l'abilitazione all'uso della stessa, comunicando la relativa accoglibilità o meno, previa verifica di congruità tecnica ed organizzativa ed evadendo le richieste nel più breve tempo possibile, compatibilmente con le proprie esigenze organizzative.

Le operazioni tecniche di cui sopra possono consistere nella semplice abilitazione dell'Utente all'accesso ed utilizzo di una risorsa informativa effettuata dal personale deputato a fornire le apposite credenziali, nel rilascio di un "account" personale ad uso esclusivo dell'Utente finale, nell'installazione sulla stazione di lavoro dell'Utente dell'opportuno programma informatico che permette l'utilizzo della risorsa informativa individuata, oppure in una combinazione di più azioni tra quelle sopra descritte.

L'Utente assegnatario di un'abilitazione all'accesso ad un qualunque sistema informativo sottoscrive la dichiarazione di presa visione ed accettazione delle norme contenute nelle presenti Norme.

Art. 17

Utilizzo

• E'assolutamente vietato all'Utente divulgare ad altri Utenti informazioni relative ad un account personale per l'accesso ed utilizzo delle risorse informative ad egli assegnate.

• E' espressamente vietato all'Utente accedere in maniera non autorizzata a banche dati accessibili tramite collegamento ai servizi di rete informatica interna o esterna, compresa Internet, nonché di effettuare, o far effettuare da terzi, l'installazione di programmi informatici su qualunque tipo di elaboratore, in particolare sulle stazioni di lavoro assegnate agli Utenti.

Le predette attività di installazione dovranno essere oggetto di esplicita richiesta e saranno eseguite di norma dal personale tecnico del SIC, salvo diversa esplicita autorizzazione da parte del SIC stesso.

• E' inoltre fatto divieto all'Utente di effettuare, o far effettuare da terzi, qualunque operazione di installazione o re-installazione di un qualunque prodotto software, anche facente parte della dotazione installata dal SIC sulla stazione di lavoro, oppure aggiuntivo rispetto ad essa. Sono altresì vietate tutte le modifiche tecniche che alterino in maniera sostanziale le funzionalità o le caratteristiche di funzionamento di programmi informatici, di archivi informatici o di banche dati accessibili tramite collegamento ai servizi di rete trasmissione dati interna o esterna, compresa Internet.

Tutte le succitate attività di modifica della configurazione definita dovranno essere oggetto di richiesta e saranno eseguite di norma dal personale tecnico del SIC, salvo diversa esplicita autorizzazione da parte del SIC stesso.

• inoltre è espressamente vietato:

- distribuire, anche via Posta Elettronica, o duplicare qualunque software o file (audio e/o video ecc.) soggetto a copyright, non rispettando i termini contrattuali contenuti nella relativa licenza d'uso oppure software prodotto da terzi per conto dall'Amministrazione;
- distribuire, anche via Posta Elettronica, qualsiasi tipo di software o file (audio e/o video ecc.) che possa danneggiare o limitare le funzionalità dei Sistemi informativi o delle Risorse Informatiche dell'Amministrazione, in particolare software virale.

L'Utente è consapevole che lasciare un elaboratore incustodito può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. Per questo motivo viene suggerito all'Utente che, prima dello spegnimento fisico della stazione di lavoro utilizzata per l'attività lavorativa oppure in caso di assenze prolungate dall'ufficio, si proceda preventivamente allo scollegamento (logout) dalla Risorsa Informativa che egli stava utilizzando.

Il SIC o personale da esso delegato (Help-desk esterno ecc.) è autorizzato a rimuovere d'ufficio ed eliminare qualsiasi software e/o file (fotografico, audio e/o video ecc.) soggetto a copyright individuato in rete c/o su strumenti informatici dell'Amministrazione, del quale l'Utente non sappia giustificarne il titolo.

Art. 18

Codici di Accesso (password)

L'accesso alle informazioni contenute negli archivi di un qualunque elaboratore deve essere protetto da codice d'accesso (altrimenti denominata: password), custodita secondo quanto previsto dall'Allegato B del D.Lgs. 30 giugno 2003, n. 196 e realizzata secondo quanto riportato nel DPS dell'Ente consultabile in una apposita area "pubblica" della intranet denominata D.Lgs. 196/03 comunicazioni.

L'Utente ha quindi l'esclusiva responsabilità di custodire la password, comunicata nella fase di abilitazione all'utilizzo della singola risorsa informativa da parte dell'Utente stesso, con la massima diligenza possibile e di non comunicarla o diffonderla a terzi.

Tutte le password di accesso ed abilitazione all'utilizzo delle risorse informative e dei programmi informatici componenti i Sistemi Informativi vengono rilasciate dal SIC individualmente all'Utente utilizzatore dietro presentazione di richiesta da parte del Responsabile di Servizio o suo delegato da cui

l'Utente dipende.

Ogni Utente, a meno che la procedura non lo permetta, è tenuto a cambiare al primo accesso la password rilasciata inizialmente dal SIC per l'accesso alla risorsa informativa al primo utilizzo della risorsa stessa e, successivamente, almeno ogni 6 mesi (in caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi) pena la perdita di validità e la disattivazione della stessa (salvo termini più stringenti stabiliti nel DPS dell'Ente soggetto a revisione annuale); è obbligo dell'Utente chiedere altresì la sostituzione della password di accesso nell'eventualità in cui egli sospetti che essa abbia perso la necessaria segretezza.

Qualora un Utente venisse a conoscenza, anche in maniera fortuita, di password assegnate ad altro Utente, è tenuto a darne immediata notizia al SIC ai fini della sollecita sostituzione.

Il SIC indica come criterio generale di scelta delle password che le stesse vengano formate da almeno 10 caratteri, siano composte da lettere maiuscole/minuscole e cifre numeriche, evitando parole riconducibili a termini di uso comune tratti dal dizionario, nomi propri o geografici e riferimenti agevolmente riconducibili all'Utente stesso (es. nome del coniuge o di familiari, luogo e data di nascita, ecc).

Il Responsabile di Servizio o suo delegato da cui l'Utente dipende è tenuto a segnalare tempestivamente al SIC ogni variazione nei diritti di accesso a applicativi e/o banche dati dell'Utente stesso.

TITOLO IV

USO DEL SERVIZIO DI POSTA ELETTRONICA

Art. 19

Generalità

La Posta Elettronica è un servizio di rete telematica disponibile per gli Utenti e costituisce uno strumento di lavoro che l'Amministrazione mette a disposizione degli stessi per migliorare la comunicazione interna ed esterna all'Ente.
Il servizio di Posta Elettronica dell'Amministrazione, permette la spedizione, la ricezione e l'inoltro di messaggi di testo o compositi tra i diversi Utenti del Sistema Informativo aziendale, ma può essere anche utilizzato per le comunicazioni da e verso l'esterno dell'Amministrazione tramite l'utilizzo della rete Internet.
All'Utente viene di norma assegnata una casella di posta elettronica così composta:

nome. cognome@comune.todi.pg.it

Oppure, nel caso si tratti di posta elettronica assegnata ad un ufficio:

denominazione dell'uffico@comune.todi.pg.it

La Posta Elettronica Certificata è sistema di comunicazione analogo alla Posta Elettronica in grado di attestare l'invio e l'avvenuta consegna di un messaggio di posta elettronica e di fornire ricevute opponibili ai terzi (Art. 1 Definizioni, Finalità e Ambito di Applicazione, nuovo C.A.D.).
La casella di posta elettronica certificata istituzionale dell'Ente è la seguente:

comune.todi@postacert.umbria.it

Art. 20

Accesso

L'accesso al servizio di Posta Elettronica è riservato ai soli Utenti, previa abilitazione da parte del SIC. - L'abilitazione per l'accesso al servizio di Posta Elettronica ed il rilascio della relativa casella di posta elettronica, avviene di norma dietro presentazione al SIC di una richiesta da parte del Responsabile di Servizio o suo delegato da cui l'Utente dipende.
Con le modalità sopra descritte, il Responsabile di Servizio o suo delegato può anche richiedere al SIC l'attivazione di "alias", "gruppi di distribuzione" o caselle di Posta Elettronica non nominative, cioè non destinate ad uso di Utenti bensì di carattere istituzionale (Sindaco, Assessore, Servizio X, ecc.), specificando la lista degli Utenti abilitati all'accesso ed utilizzo della stessa.
Il SIC, ricevuta la richiesta di attivazione del servizio di Posta Elettronica per un Utente o per un gruppo di utenti, provvede in alcuni casi al rilascio di un account personale (ID utente) provvisto della relativa password di accesso ed alla creazione della casella di Posta Elettronica Istituzionale. Con le stesse modalità e dopo valutazione di opportunità tecnica, il SIC può procedere ad abilitare gli utenti ad accedere "dall'esterno" ai sistemi di posta interna dell'Ente.
L'Utente è responsabilizzato sul fatto che, nel caso di casella di posta nominale, l'ID personale rilasciato dal SIC coincide con l'account di accesso al sistema informativo (Dominio) dell'Ente e come tale soggetto alle prescrizioni di cui al precedente art. 14 e a quanto previsto dal DPS dell'Ente, e che tale account univoco attesta la riconducibilità per via analogica al redattore del messaggio e-mail. Stessa logica organizzativa si adotta nel caso dei gruppi di distribuzione o degli alias. L'accesso al servizio di Posta Elettronica Certificata Istituzionale avviene per mezzo del Sistema di Protocollo Informatico dell'Ente. Attraverso il profilo di abilitazione previsto dal proprio Responsabile di Servizio o suo delegato, nel rispetto di quanto previsto nel Regolamento del Protocollo vigente, il SIC provvede ad autorizzare l'Utente, impiegando lo stesso account di accesso al sistema informativo (Dominio) ID personale.

Art.21

Utilizzo

L'Utente si impegna ad utilizzare la casella di Posta Elettronica unicamente per scopi attinenti la propria attività lavorativa e ne risponde civilmente, penalmente e dal punto di vista disciplinare, in caso di abuso.

La dimensione massima di un singolo messaggio di Posta Elettronica in spedizione o in ricezione (compresi eventuali documenti allegati) è fissata dal SIC, anche in funzione delle caratteristiche tecniche dei sistemi. La dimensione massima dello spazio di memorizzazione per tutti i messaggi di Posta Elettronica dell'Utente, contenuti cioè nelle cartelle dei messaggi arrivati, spediti, in bozza, ecc, è anch'essa fissata dal SIC.

Il SIC si riserva di valutare dal punto di vista tecnico-organizzativo le eventuali richieste da parte degli Utenti di aumento delle dimensioni della casella di Posta Elettronica. E' precisa responsabilità dell'Utente:

- evitare l'utilizzo della Posta Elettronica per lo scambio documenti (file) tra i diversi uffici dell'Ente, utilizzare per tale scopo gli spazi di rete condivisi nella Intranet, limitandosi ad inviare via e-mail soltanto la comunicazione relativa alla disponibilità del file;
- tenere in ordine la casella di Posta Elettronica, curando periodicamente la dimensione della stessa (sia documenti arrivati che spediti), cancellando o archiviando i documenti inutili oppure obsoleti, soprattutto se dotati di allegati voluminosi.

È responsabilità dell'Utente controllare, in particolar modo prima della spedizione, che eventuali documenti allegati ad un messaggio di Posta Elettronica non siano affetti da virus informatici.

E espressamente vietato utilizzare il servizio di Posta Elettronica per:

- inoltrare o ricevere messaggi di carattere personale durante l'orario di lavoro;
- inviare o memorizzare messaggi interni o esterni di natura oltraggiosa, discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale o partitica;
- partecipare a dibattiti, forum o mailing list non aventi attinenza con l'attività lavorativa;
- partecipare alle cosiddette "catene telematiche" (altresì denominate "catene di S. Antonio") - inviare a gruppi di utenti, interni e/o esterni, messaggi non richiesti (Spamming).

L'utente può ricevere ed inoltrare messaggi di carattere personale, purché ciò avvenga:

- senza alcun costo aggiuntivo a carico del Comune di Todi;
- al di fuori dell'orario di lavoro (per esempio, durante la "pausa pranzo").

La congruità e la variabilità dei succitati requisiti verrà valutata, su eventuale segnalazione del SIC, dal Sindaco. I sistemi di webmail forniti da Internet Service Provider esterni (hotmail, katamail, virgilio, ecc.) sono inibiti dalle policy di sicurezza dell'Ente.

Il SIC assicura la riservatezza dei contenuti delle caselle definite sistema di Posta Elettronica interno adottando opportune misure a garanzia della sicurezza informatica dei sistemi; resta però responsabilità dell'Utente curare la riservatezza della visione di comunicazioni contenute nella propria casella di Posta Elettronica, proteggendo opportunamente l'accesso indebito da parte di terzi alla stazione di lavoro come prescritto all'art. 1 delle presenti Norme.

E possibile per l'Utente utilizzare la conferma dell'avvenuta consegna del messaggio spedito ad un destinatario interno del servizio di Posta Elettronica (altresì chiamata: ricevuta di ritorno); in dipendenza però delle diverse caratteristiche dei sistemi di Posta Elettronica utilizzati dai possibili corrispondenti esterni dell'Amministrazione, non potrà sempre essere assicurata all'Utente interno la conferma di ricezione di un messaggio spedito all'esterno dell'Amministrazione. In caso di invio di messaggi di posta all'esterno dell'Ente, l'utente dovrà inserire in calce all'e-mail il "disclaimer" che può assumere la seguente forma:

Disclaimer:

L'invio di questa e-mail è destinato solo ad uso personale o a enti sopra nominati e potrebbe contenere informazioni riservate, coperte da segreto professionale, e non soggette a divulgazione ai sensi di legge. Se non ne siete i corretti destinatari, con la presente siete informati che non vi è assolutamente permessa alcuna divulgazione, copia, distribuzione, o altro uso delle informazioni in essa contenute. Se per errore avete ricevuto questo messaggio, Vi chiedo cortesemente di informarmi

mmediatamente al mio indirizzo di posta elettronica. Grazie CONFIDENTIALITY NOTICE his message and its attachments are addressed solely to the persons above and may ontain confidential information. If you have received the message in error, be nformed that any use of the content hereof is prohibited. Please return it mmediately to the sender and delete the message. Should you have any questions, lease contact us by replying to my e-mail address. Thank you.

Gli utenti sono edotti che tutto il traffico inerente il servizio di Posta Elettronica interna dell'Ente è egistrato in forma analitica (ivi compresi quindi il contenuto dei messaggi. i dati esteriori della comunicazione d i file allegati) per le motivazioni e con le modalità di cui al precedente art. 4 e che eventuali forme di ontrollo sul rispetto del corretto uso degli strumenti di lavoro e dell'effettivo adempimento della prestazione avorativa avverranno esclusivamente secondo quanto indicato al precedente art. 5 ed ai sensi della leliberazione del Garante della Privacy n.13 del 1.03.2007 e della Direttiva N°02/09 del 26/05/2009 della 'residenza del Consiglio, Dipartimento della Funzione Pubblica avente ad oggetto "l'utilizzo di internet e della asella di posta elettronica istituzionale sul luogo di lavoro".

Essendo stato appositamente e chiaramente specificato l'uso istituzionale e non personale delle caselle di posta ssegnate dall'Ente agli utenti, resta quindi esclusa qualsiasi aspettativa di confidenzialità da parte degli tilizzatori di tale sistema di comunicazione lavorativa.

Ciononostante al fine di prevenire l'apertura della posta elettronica dei singoli utenti, viene messa a disposizione li ciascun lavoratore una apposita funzionalità all'interno del sistema di posta dell'Ente, di agevole utilizzo, he consente di inviare automaticamente, in caso di assenza (ferie, lavoro fuori sede, ecc.) , messaggi di posta ontenenti le "coordinate" elettroniche o telefoniche (indirizzi e-mail o numeri telefono) di un altro soggetto o altre modalità di contatto del servizio in cui opera. In caso di eventuale assenza non programmata (ad es. per nalattia), qualora il lavoratore non possa attivare la procedura suddetta, e stante il perdurare dell'assenza oltre un accettabile limite temporale, l'Amministrazione può disporre lecitamente, in caso di necessità, di attivare analogo accorgimento tramite il personale del SIC, dandone comunicazione agli interessati. In previsione inoltre della possibilità che, in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa e istituzionale dell'Ente, si debba conoscere il contenuto dei messaggi di posta elettronica, l'interessato è invitato a delegare altro lavoratore (fiduciario) a verificare il contenuto dei messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa e istituzionale. A cura del titolare del trattamento, di tale attività può essere redatto apposito verbale e/o informare il lavoratore interessato alla prima occasione utile.

TITOLO V

USO DEL SERVIZIO DI RETE INTERNET

Art. 22

Generalità

La rete Internet è una risorsa informativa esterna che l'Amministrazione mette a disposizione degli Utenti per la ricerca di informazioni sul web e per migliorare la qualità del lavoro svolto negli uffici comunali. L'accesso e l'utilizzo del servizio di rete Internet è riservato esclusivamente per scopi attinenti l'attività lavorativa degli Utenti. L'Utente è responsabilizzato sul fatto che taluni utilizzi impropri della rete Internet possono mettere a rischio la sicurezza informatica dei Sistemi Informativi.

Art. 23

Accesso

L'accesso al servizio di rete Internet è attualmente a disposizione di tutti gli Utenti aventi un account di accesso al Dominio (c.d. collegamento in rete).

Art. 24

Utilizzo

E' vietata la consultazione e la navigazione sui siti della rete Internet per motivi diversi da quelli strettamente legati all'attività lavorativa svolta dall'Utente. E' assolutamente vietato scaricare dalla rete Internet sulla stazione di lavoro assegnata all'Utente o su qualsiasi tipo di supporto di memorizzazione qualunque tipo di materiale o file (audio e/o video ecc.) soggetto a copyright, ad eccezione di quello avente attinenza con l'attività lavorativa dell'Utente per il quale l'Ente dispone dei diritti di utilizzazione.

Per materiale non scaricabile da Internet si intende, ad esempio:

- archivi o banche dati contenenti informazioni testuali, immagini, musica, video soggetti a copyright file musicali, immagini o video ancorché gratuiti;
- programmi informatici, in particolare quelli eseguibili sulla stazione di lavoro assegnata all'Utente come ad esempio salva schermo o prodotti software sia freeware che su licenza, salvo esplicita autorizzazione da parte del SIC;

E' tassativamente vietata l'effettuazione di attività ludiche e di ogni genere e di transazione finanziaria ad uso personale.

L'Utente è responsabilizzato sul fatto che la registrazione, se non strettamente necessario, dei propri dati personali (ivi compreso l'indirizzo della casella di Posta Elettronica rilasciato dal SIC), su siti Internet non sicuri non è raccomandabile per motivi di sicurezza informatica.

E' vietata la partecipazione a forum non professionali, l'utilizzo di chat line, di bacheche elettroniche, le registrazioni in "guest-books" (anche utilizzando pseudonimi) e quant'altro in generale possa ricadere nella fattispecie di uso a scopi personali della rete Internet. Allo scopo di ridurre il rischio di usi impropri della "Navigazione" in internet, minimizzando così la necessità di operare successivi controlli sui lavoratori, è presente nei sistemi informativi dell'Ente un "proxy server" con finalità di filtro dei contenuti, consentendo quindi la .

Tale software previene (con possibilità di errore sia di falsi positivi che di falsi negativi) il download o l'upload di file aventi particolari caratteristiche dimensionali o di tipologia di dato e l'accesso a siti reputati incongruenti con l'attività lavorativa mediante suddivisione per macrocategorie.

Qualora per esigenze lavorative si riscontri la necessità di richiedere modificazioni alla configurazione impostate dal SIC sul sistema, dovrà essere inoltrata a quest'ultimo apposita richiesta formale (anche mediante lo strumento della posta elettronica). Gli utenti sono edotti che il traffico inerente la navigazione in Internet effettuata tramite la rete telematica comunale è registrato in forma analitica sui server

aziendali ivi compresi i siti visitati, per un tempo massimo di quarantotto ore allo scopo di consentire la raccolta delle informazioni utili al controllo dell'utilizzo del servizio di rete internet stessa. Successivamente il sistema di controllo della navigazione (Proxy Server) provvederà in forma anonima alla raccolta e alla archiviazione di log file riferiti a Blocking-event Reports (registrazione eventi di blocco) per: Riskiest URLs by viruses detected (indirizzi bloccati per accertati motivi di virus), Most blocked URL categories (siti bloccati perché categorizzati come non appartenenti a quelli istituzionali) Most blocked URLs (siti maggiormente bloccati). Per tipologie di infezioni registrate: Spyware/Grayware Reports, Top spyware/grayware detections, top users with Spyware/Grayware Infections.

Per le motivazioni e con le modalità di cui al precedente art. 4, eventuali forme di controllo sul rispetto del corretto uso degli strumenti di lavoro e dell'effettivo adempimento della prestazione lavorativa, avverranno esclusivamente secondo quanto indicato al precedente art. 5 ed ai sensi della deliberazione del Garante della Privacy n.13 del 1.03.2007.

USO DEI SERVIZI DI TELEFONIA FISSA E MOBILE

Art. 25
Generalità

I Servizi facenti parte della Rete Telefonica dell'Amministrazione assegnabili agli Utenti vengono di norma erogati da Risorse strumentali appartenenti alla Rete Telefonica Fissa (tipicamente le postazioni telefoniche da tavolo) ed apparati di Rete Telefonica Mobile (apparati radiomobili cellulari), nonché software per la telefonia VOIP.
Le Risorse di cui sopra vengono assegnate all'Utente in ragione dello svolgimento dell'attività lavorativa e delle funzioni a essa strettamente inerenti, in modo da rispondere all'interesse e alle esigenze dell'Amministrazione ed al miglioramento della qualità del lavoro e della produttività individuale.
In questo contesto, qualunque impiego di Risorse di Rete Telefonica Fissa deve essere considerato ai soli scopi lavorativi e comunque in un quadro di corretto controllo della spesa corrente e miglioramento dell'efficienza interna dell'Amministrazione.
L'Amministrazione si conforma, in via di applicazione analogica, per l'accesso ed utilizzo dei sistemi e delle apparecchiature di telefonia fissa e mobile, ai principi di cui alle lettere a), b) e e) del comma 1 dell'art. 2 delle direttive approvate con D.P.C.M. 11 aprile 1997.

Art. 26
Accesso alle Risorse di Rete Telefonica Fissa

L'accesso alle Risorse di Rete Telefonica Fissa è riservato ai soli Utenti, previa assegnazione delle stesse da parte del SIC.
L'assegnazione della Risorsa ad un Utente avviene di norma dietro presentazione di una richiesta motivata da parte del Responsabile di Servizio o suo delegato da cui l'Utente dipende, che evidenzia anche il profilo di autorizzazione richiesto in considerazione del ruolo e delle funzioni svolte da parte dell'Utente.
Di norma ogni apparato di rete telefonica fissa viene assegnato nominalmente a un Utente oppure, qualora si tratti di Risorsa condivisa da più Utenti non assegnabile individualmente, al Responsabile dell'ufficio ovvero al Responsabile di Servizio o suo delegato dal quale egli dipende.
Il SIC ricevuta la richiesta di assegnazione della Risorsa, effettua la verifica di fattibilità, comunicando entro 7 giorni lavorativi dalla richiesta la relativa accoglibilità o meno, provvedendo successivamente di norma all'acquisizione ed assegnazione fisica della stessa sul posto di lavoro dell'Utente ed all'attivazione di una nuova utenza telefonica (numero interno).

Il SIC provvede all'evasione delle richieste nel più breve tempo possibile, di norma nel rispetto dell'ordine di arrivo delle stesse e tenendo in debito conto le situazioni organizzative e le esigenze debitamente segnalate che impongono particolare urgenza, riservandosi la facoltà di considerare l'effettiva esigenza della richiesta in relazione alle possibili alternative ed alla disponibilità di numeri interni.

Art. 27
Utilizzo delle Risorse di Rete Telefonica Fissa

Pur ribadendo l'uso ai soli fini lavorativi dell'apparecchiatura telefonica, è consentito l'utilizzo in via eccezionale dello stesso anche ai fini privati per motivate esigenze inderogabili ed indifferibili.
In ogni caso è espressamente vietato ad un Utente l'utilizzo ai fini privati di un apparato telefonico assegnato ad altro Utente. I controlli sulle risorse telefoniche verranno effettuati ai sensi dell'Art. 5 del

presente regolamento. A tutela dell'Amministrazione, il SIC si riserva la facoltà di verificare dagli appositi tabulati telefonici forniti dalle apparecchiature di Rete Telefonica Fissa o dal provider di connettività il flusso di traffico uscente da un apparato telefonico assegnato ad un Utente, anche dietro presentazione di richiesta motivata da parte del Responsabile di Servizio o suo delegato da cui l'Utente dipende, assolvendo in tal modo alla funzione di controllo mirato rispetto all'utilizzo dell'apparecchio.

Il SIC si riserva inoltre di effettuare d'ufficio tutti i controlli del caso qualora dall'esame del traffico telefonico relativo alle utenze attive venga rilevato uno scostamento significativo dalla media rilevata in precedenza.

Art. 28

Impiego Risorse di Rete Telefonica Mobile

Per la disciplina relativa si rinvia al regolamento approvato con Deliberazione di Giunta Comunale n°340 del 21.12.2006

TITOLO VII

DISPOSIZIONI FINALI

Art. 29

Responsabilità degli Utenti

Ciascun Utente dei Sistemi Informativi ha la responsabilità di segnalare immediatamente al SIC ogni sospetto di effrazione, incidente, abuso o violazione della sicurezza riguardante le Risorse Informatiche, Telematiche e Telefoniche ad egli assegnate o comunque utilizzate.
In particolar modo ogni utente è consapevole che di qualsiasi forma di risorsa *hardware o software* in sua disponibilità o installata su risorse in sua disponibilità (ad es. programmi software non licenziati, modem analogici, ecc), se non espressamente indicata nell'elenco di cui alla "Dichiarazione di accettazione" da egli controfirmata, risponderà personalmente a livello disciplinare e amministrativo oltreché per ogni eventuale risvolto giuridico civilistico e penale.
Ciascun utente si assume inoltre la responsabilità di individuare autonomamente la miglior ubicazione per la postazione di lavoro ed ogni altra risorsa ad egli assegnata, al fine di ridurre il rischio di impieghi abusivi. Il mancato rispetto o la violazione delle regole contenute nelle presenti Norme costituisce illecito perseguibile disciplinarmente, fatte salve le responsabilità civili e penali.
Si ribadisce inoltre che l'Amministrazione, ai sensi delle disposizioni riportate al Titolo 1 del presente disciplinare, si riserva di attivare controlli mirati a scoprire utilizzi di Internet , di posta elettronica e di telefonia scorretti. Si precisa comunque che ai fini disciplinari le presenti Norme vengono pubblicate sul sito istituzionale del Comune di Todi, come previsto dall'art. 7, legge 20 maggio 1970, n. 300 (Statuto dei lavoratori) e sul server dell'Ente. Si precisa, inoltre, che, ai fini degli obblighi di preventiva informazione ai sensi dello Statuto dei lavoratori e del D.Lgs. 196/2003, la pubblicazione del presente regolamento costituisce, a tutti gli effetti, "informazione preventiva" generale per tutti i dipendenti, e, in quanto tale, legittimante i controlli di cui all'art. 5 e al precedente art. 27. Si informa infine che ai fini dell'esercizio dei propri diritti (art. 7 D.Lgs. 196/2003) il lavoratore può rivolgersi direttamente al "Titolare del trattamento" nella persona del Sindaco protempore (Art. 29 D.Lgs.196/2003).