COMUNE DI ARIANO IRPINO

(Provincia di Avellino)

REGOLAMENTO

SERVIZIO

INFORMATICO

COMUNALE

Indice

Premessa

La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete Internet dai Personal Computer, espone *la Rete del Comune di Ariano Irpino e i suoi dipendenti* a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (legge sul diritto d'autore e legge sulla privacy, fra tutte), creando evidenti problemi alla sicurezza ed all'immagine dello stesso Comune.

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

Le prescrizioni di seguito previste si aggiungono ed integrano le specifiche istruzioni già fornite a tutti gli incaricati in attuazione del D. Lgs. 30 giugno 2003 n. 196 e del Disciplinare tecnico (Allegato B al citato decreto legislativo) contenente le misure minime di sicurezza, nonché integrano le informazioni già fornite agli interessati in ordine alle ragioni e alle modalità dei possibili controlli o alle conseguenze di tipo disciplinare in caso di violazione delle stesse.

Inoltre questo regolamento segue le linee guida tracciate dal Codice dell'Amministrazione Digitale (D. Lgs. n. 82/2005) e s.m.i. che stabilisce le regole per la digitalizzazione della pubblica amministrazione.

È necessario mettere a disposizione delle Amministrazioni e dei pubblici dipendenti strumenti (soprattutto digitali) in grado di incrementare l'efficienza e l'efficacia dell'intero sistema pubblico.

Il Gruppo di Lavoro costituito per la riorganizzazione del Servizio Informatico Comunale con delibera di G. C. n. 55 del 1 marzo 2013, è incaricato di seguire e rendere possibile, con le azioni che le normative ed il CAD consentono, piena esigibilità ai servizi forniti dall'Amministrazione Pubblica, contribuendo a sburocratizzare, semplificando il dialogo della PA con i cittadini e imprese, riducendo i costi di funzionamento della Amministrazione Pubblica rendendo in tal modo più efficiente il sistema produttivo.

1. Oggetto, ambito di applicazione, riferimenti normativi

1.1 Il presente regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori del Comune a prescindere dal rapporto contrattuale con lo stesso intrattenuto (lavoratori somministrati, collaboratori a progetto, in stage, ecc.) ed a chiunque dovesse utilizzare le risorse informatiche del Comune di Ariano Irpino.

1.2 Incaricati del controllo sul rispetto e l'esecutività di questo Regolamento Comunale sono il Responsabile del Servizio Informatico Comunale (di seguito: Responsabile S.I.C.) ed i componenti del Gruppo di Lavoro del S.I.C. (delibera di G. C. n. 55 del 1 marzo 2013) nel rispetto della privacy degli utenti.

1.3 Il presente regolamento è stato redatto tenendo conto delle linee guida del Garante della Privacy D.Lgs 196/03 e s.m.i., del Codice dell'Amministrazione Digitale D. Lgs. n. 82/2005) e s.m.i. oltre che delle "Linee Guida del Garante per posta elettronica e internet" del 1 marzo 2007 e del provvedimento del 27 novembre 2008 recante "Misure ed accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di Sistema".

1.4 Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi ogni utilizzatore incaricato a cui vengono concesse specifiche credenziali di autenticazione e che ha accesso ad una postazione Personal Computer collegata alla rete comunale.

1.5 In riferimento al Documento Programmatico Sicurezza già redatti ed approvati, il titolare della privacy nomina i responsabili della privacy i quali a loro volta nominano gli utenti incaricati del trattamento dei dati.

Il Responsabile S.I.C. nomina gli amministratori di sistema per le procedura informatiche, sentiti i Responsabili della Privacy.

2. Utilizzo del Personal Computer

2.1 Il Personal Computer assegnato al dipendente è uno strumento di lavoro. Esso permette l'accesso alla rete del Comune di Ariano Irpino solo attraverso specifiche credenziali di autenticazione, come meglio descritto al successivo punto 4 del presente Regolamento. Ogni utilizzo non inerente l'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e soprattutto, minacce alla sicurezza. Il Personal Computer deve essere custodito con cura evitando ogni possibile forma di danneggiamento.

2.2 L'accesso all'elaboratore deve essere protetto da password custodita dall'utente con la massima diligenza e non divulgata. La stessa password deve essere attivata per l'accesso alla rete, per l'accesso a qualsiasi applicazione, per lo "screen saver" e per il collegamento a Internet.

2.3 Il personale incaricato del S.I.C. ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni Personal Computer al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc. L'intervento viene effettuato su chiamata dell'utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione dell'intervento.

2.4 Non è consentito l'uso di programmi diversi da quelli ufficialmente e legalmente installati per conto del Comune, né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. L'inosservanza della presente disposizione espone lo stesso Ente e l'utilizzatore a gravi responsabilità civili. Si evidenzia inoltre che le violazioni della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, vengono sanzionate anche penalmente.

2.5 Non è consentito all'utente modificare le caratteristiche (hardware, software, impostazioni di sistema, Ip adress, ecc…) impostate sul proprio Personal Computer. Qualsiasi intervento di modifica delle caratteristiche di cui sopra, è demandato al S.I.C.

2.6 Il Personal Computer deve essere spento sempre prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. In ogni caso è vietato lasciare un elaboratore incustodito connesso alla rete.

2.7 L'utente deve mettere in atto accorgimenti tali per cui il computer non resti, durante una sessione di trattamento:

- incustodito: può essere sufficiente che un collega rimanga nella stanza, durante l'assenza di chi sta lavorando con lo strumento elettronico, anche se la stanza rimane aperta.

- e accessibile: può essere sufficiente attivare lo screen saver con password oppure chiudere a chiave la stanza, dove è situato lo strumento elettronico, durante l'assenza, anche se nella stessa non rimane nessuno.

2.8 Non è consentita l'installazione sul proprio Personal Computer di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, switch, ecc.), se non con espressa autorizzazione del Responsabile S.I.C.

2.9 Agli utenti incaricati del trattamento dei dati sensibili o giudiziari è fatto divieto l'accesso contemporaneo con lo stesso account da più Personal Computer.

2.10 Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il personale S.I.C. nel caso in cui siano rilevati virus ed adottando quanto previsto dal successivo punto 11 del presente Regolamento relativamente alle procedure di protezione antivirus.

2.11 Non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

2.12 L'eventuale malfunzionamento o danneggiamento del personal computer e di ogni altra dotazione informatica deve essere tempestivamente comunicato, per il tramite del proprio Responsabile di Servizio e/o Dirigente di Area al Responsabile S.I.C.

2.13 In caso di furto o accesso fraudolento è onere dell'utente effettuare denuncia all'autorità di polizia e far pervenire al Responsabile S.I.C. copia della denuncia.

2.14 E' compito di ciascun Responsabile di Servizio e/o Dirigente di Area compartecipare al processo di gestione della sicurezza informatica e collaborare con il Responsabile S.I.C., alla verifica del

corretto utilizzo delle risorse assegnate, allo scopo di evitarne sia l'uso improprio, sia l'accesso da parte di personale non autorizzato.

3. Utilizzo della rete

3.1 Le unità di rete sono aree di condivisione di informazioni strettamente lavorative dell'ente e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità, vengono svolte regolari attività di controllo, amministrazione e backup da parte del Personale S.I.C.

3.2 Per l'accesso alla rete del Comune di Ariano Irpino ciascun utente deve essere in possesso delle specifiche credenziali di autenticazione. Le password d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite. E' assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione utente di un altro operatore.

3.3 Sentito il Responsabile del servizio e l'utente, il Personale S.I.C. può procedere alla rimozione di ogni file o applicazione che riterrà pericoloso per la sicurezza sia sui Personal Computer degli utenti sia sulle unità di rete.

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

3.5 E' cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria, ritirandola prontamente dai vassoi delle stampanti comuni. E' buona regola evitare di stampare documenti o file non adatti (*molto lunghi o non supportati, come ad esempio il formato pdf o file di contenuto grafico*) su stampanti comuni. In caso di necessità la stampa in corso può essere cancellata.

3.6 Ogni apparecchiatura collegata alla rete comunale senza la preventiva autorizzazione del Responsabile S.I.C. sarà ritenuta compromettente e dannosa per la qualità del servizio, anche se correttamente applicata. Spetterà al Responsabile S.I.C. valutarne l'opportunità dell'operazione.

4. Gestione ed assegnazione delle credenziali di autenticazione

4.1 Le credenziali di autenticazione per l'accesso alla rete comunale, sono attribuite dal personale del Servizio Informatico e successivamente resettate e personalizzate dal dipendente stesso secondo criteri prestabiliti.

4.2 Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id), assegnato dal S.I.C., associato ad una parola chiave (password) riservata e creata dall'incaricato che dovrà essere memorizzata, custodita con la massima diligenza, non divulgata. Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte del personale S.I.C. La parola chiave deve essere formata da 8 o più caratteri appartenenti ad almeno tre delle seguenti quattro categorie: lettere maiuscole, lettere minuscole, numeri, caratteri speciali, anche in combinazione fra loro e non deve contenere riferimenti agevolmente riconducibili all'incaricato.

4.3 La password deve essere segreta e quindi non conoscibile da terzi.

4.4 La password di accesso di ciascun utente sarà automaticamente resettata ogni tre mesi. In base a tale procedura automatica, l'utente, mediante avviso a video, dovrà inserire ogni 3 mesi una password nuova, diversa dalla precedente.

4.5 Soggetto preposto alla custodia delle credenziali di autenticazione è il personale S.I.C. del Comune di Ariano Irpino.

4.6 Nessuno, neppure il Titolare del trattamento, può accedere allo strumento elettronico, utilizzando la credenziale di autenticazione dell'utente. Eccezione a tale regola si ha solo se si verificano congiuntamente le seguenti condizioni:

- prolungata assenza o impedimento dell'utente

- l'intervento è indispensabile e indifferibile

- vi sono concrete necessità, di operatività e di sicurezza del sistema.

A tale fine, gli utenti dovranno:

- predisporre una copia della parola chiave, provvedendo quindi a trascriverla su un foglio, facendo però in modo che l'informazione resti segreta, ed inserendola in una busta chiusa;

- predisporre e consegnare tale copia al Custode delle Password, che sia stato previamente incaricato della sua custodia. Solo al verificarsi delle condizioni sopra esposte, il titolare o un responsabile potranno richiedere la busta che la contiene, al Custode delle Password.

Rientrano tra i compiti del Custode:

- conservare in luogo sicuro e chiuso a chiave le buste contenenti le password;

- provvedere ad informare, tempestivamente e per iscritto, l'incaricato cui appartiene la parola chiave, dell'accesso effettuato;

- verificare la regolare consegna nei tempi previsti (sei o tre mesi) delle buste con le nuove password da parte degli incaricati.

4.7 La password deve essere immediatamente sostituita, dandone comunicazione al Custode delle Password, nel caso si sospetti che la stessa abbia perso la segretezza.

4.8 Qualora l'incaricato venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia al Responsabile S.I.C.

4.9 Il codice per l'identificazione (user-id), che l'Amministratore del Sistema provvede a fornire all'utente, quale componente della chiave per accedere all'elaboratore e successivamente a gestire, deve essere univoco: esso non può essere assegnato ad altri utenti, neppure in tempi diversi.

4.10 Le credenziali di autenticazione (password e user-id) devono essere disattivate nei seguenti casi:

- immediatamente, nel caso in cui l'utente perda la qualità che gli consentiva di accedere allo strumento: ciò non accade solo se la persona cessa di lavorare, ma può ad esempio avvenire anche se l'utente viene trasferito da un ufficio all'altro, con conseguente cambio delle mansioni e degli ambiti di trattamento dei dati personali, che rendesse necessaria l'attribuzione di una nuova chiave;

- in ogni caso, entro sei mesi di mancato utilizzo. Fa ovviamente eccezione il caso delle chiavi che sono state preventivamente autorizzate per soli scopi di gestione tecnica, il cui utilizzo assume generalmente caratteristiche di sporadicità (ad esempio, potrebbero essere utilizzate solo una volta l'anno, nel quadro della verifica globale, sulla funzionalità complessiva del sistema).

4.11 Qualora i Personal Computer assegnati non siano tecnicamente configurati alla gestione esterna delle password, l'utente è responsabile del rispetto delle succitate disposizioni. Le credenziali di autenticazione (password e user-id) di software proprietari esterni e non attribuite direttamente dal S.I.C. devono avere le medesime caratteristiche di quelle di rete e devono essere soggette agli stessi principi fondamentali di sicurezza.

5. Utilizzo e conservazione dei supporti rimovibili

5.1 Tutti i supporti magnetici riutilizzabili (hard disk portatili, penne USB, dischetti, cassette, CD-DVD, cartucce, ecc…) contenenti dati personali o sensibili devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato. Una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione.

5.2 I supporti magnetici riutilizzabili (hard disk portatili, penne USB, dischetti, cassette, CD-DVD, cartucce, ecc…) contenenti dati personali o sensibili devono essere custoditi ed utilizzati in modo tale da impedire accessi non autorizzati (furti inclusi) e trattamenti non consentiti.

5.3 Una volta cessate le ragioni per la conservazione dei dati, i supporti non possono venire abbandonati, ma si devono porre in essere gli opportuni accorgimenti, finalizzati a rendere inintelligibili e non ricostruibili tecnicamente i dati in essi contenuti, al fine di impedire che essi vengano carpiti da persone non autorizzate al trattamento. Si devono quindi cancellare i dati, se possibile, o arrivare addirittura a distruggere il supporto, se necessario.

5.4 I supporti magnetici contenenti dati personali e sensibili devono essere custoditi in archivi chiusi a chiave.

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

5.6 Tutti i file di provenienza incerta od esterna, ancorché attinenti all'attività lavorativa, devono essere sottoposti al controllo ed alla relativa autorizzazione all'utilizzo.

5.7 Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il Responsabile S.I.C. nel caso in cui siano rilevati virus ed adottando quanto previsto dal presente Regolamento relativo alle procedure di protezione antivirus.

5.8 Nel caso di utilizzo Personal Computer portatili accessibili per mezzo di smart card o tessere magnetiche in possesso a proprio uso esclusivo, ogni incaricato dovrà conservare (es. non abbandonandole sulla scrivania) e proteggere (es. non avvicinarle a fonti di calore) tali dispositivi con la massima cura. Per tutelarsi in caso di furto, è altresì necessario, per l'accensione del relativo strumento elettronico, associare a tali dispositivi una password.

6. Utilizzo di PC portatili - tablet

6.1 L'utente è responsabile del Personal Computer portatile o tablet assegnatogli dal Personale S.I.C. e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

6.2 Ai Personal Computer portatili o tablet si applicano le regole di utilizzo previste dal presente Regolamento come per i Personal Computer connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.

6.3 Particolare diligenza deve essere posta dall'utente di Personal Computer portatile o tablet utilizzato in ambienti esterni all'Amministrazione, sia sotto il profilo della protezione dell'apparecchiatura, sia sotto il profilo della sicurezza dei dati in essa contenuti.

6.4 E' vietato connettersi alla rete comunale attraverso qualsiasi dispositivo personale (Personal Computer portatile, tablet, smartphone ...) non preventivamente autorizzato dal S.I.C.

7. Salvataggio e ripristino dei dati

7.1 I dati devono essere salvati con cadenza settimanale. Ogni utente è tenuto a controllare il regolare funzionamento dei back up, anche se fatto a livello di server, e verificare il salvataggio dei file inerenti l'attività lavorativa presenti nel proprio Personal Computer.

7.2 Per i dati sensibili o giudiziari l'utente deve essere in grado di provvedere al ripristino dei dati entro sette giorni.

8. Uso della posta elettronica

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

8.2 Le caselle di posta elettronica sono accessibili a tutti i dipendenti comunali specificando, in caratteri minuscoli, un identificativo costituito dalla "prima lettera del proprio nome" + "." + "cognome"+ "@comunediariano.it"(per es. Mario Rossi accederà con m.rossi@comunediariano.it).

8.3 È fatto divieto di utilizzare le caselle di posta elettronica per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica per:

- l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es.mp3) non legati all'attività lavorativa;

- l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list non legati all'attività lavorativa;

- la partecipazione a catene telematiche o spam. Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.

8.4 E' buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi. La casella di posta deve essere, a cura dell'utente assegnatario mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

8.5 Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per l'Amministrazione Comunale, ovvero contenga documenti da considerarsi riservati in quanto contraddistinti dalla dicitura "strettamente riservati" o da analoga dicitura, deve essere visionata od autorizzata. In ogni modo, è opportuno fare riferimento alle procedure in essere per la corrispondenza ordinaria.

8.6 Per la trasmissione di file tra gli uffici è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati.

8.7 E' obbligatorio controllare i file attachements di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

8.8 E' vietato inviare catene telematiche (o di Sant'Antonio). Se si dovessero ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al personale S.I.C. Non si deve in alcun caso attivare gli allegati di tali messaggi.

8.9 Nel caso in cui un utente di posta si assenti per più giorni (p.es. per malattia), sarà consentito al superiore gerarchico dell'utente incaricato o comunque, sentito l'utente, a persona individuata dall'Ente, accedere alla casella di posta elettronica, al fine di garantire la continuità del Servizio lavorativo e comunque nel rispetto del principio di necessità, di proporzionalità e privacy. L'utente al suo rientro dovrà provvedere a cambiare la password di accesso alla sua casella mail.

9. Uso della Posta Elettronica Certificata - PEC

9.1 La **Posta Elettronica Certificata** (di seguito: **PEC)** è un sistema di trasporto di documenti informatici. Consente di certificare l'invio, l'integrità e l'avvenuta consegna del messaggio. Ha lo stesso valore legale della raccomandata con avviso di ricevimento garantendo il possessore della **PEC** verso terzi dell'avvenuta spedizione del messaggio e dell'eventuale allegata documentazione. La **PEC** è quindi simile per funzionamento ad una posta elettronica convenzionale, ma è organizzata in modo da dare garanzie certe sul processo di trasmissione.

9.2 Nella Amministrazione Pubblica, così come previsto dal CAD, ogni casella di **PEC** è istituita per il registro di protocollo generale dell'Ente; l'indirizzo di **PEC** è reso pubblico sulla home page del proprio sito; l'indirizzo di **PEC** è reso pubblico sul portale Governativo ***www.indicepa.gov.it*****;** è obbligo utilizzare la PEC con tutti gli utenti che ne facciano richiesta, senza poter addurre difficoltà tecnologiche ed organizzative per impedire l'esercizio di questo diritto.

9.3 Il valore legale della comunicazione via **PEC** equivale a quello di un invio effettuato tramite raccomandata A/R.

9.4 Le informazioni che l'Amministrazione scambia attraverso messaggi di **PEC,** devono essere trattate alla stessa stregua di quelle scambiate attraverso i canali di comunicazione tradizionali. Ne consegue la necessità di indirizzare il flusso di e-mail relativo alle caselle di **PEC** sullo stesso sistema

di protocollazione utilizzato per i documenti tradizionali. E' pertanto preferibile adottare prodotti di gestione del Protocollo Informatico predisposti per il trattamento dei messaggi e degli allegati veicolati via **PEC** o soluzioni in grado di collegare il sistema di gestione della posta elettronica di tipo **PEC** e quello di gestione del protocollo.

9.5 La PEC è utilizzata: per **mandare documenti** a Enti e Pubbliche Amministrazioni; per i **rapporti tra imprese, cittadini e Pubblica Amministrazione**; per lo scambio di offerte, ordini, contratti, gare d'appalto; per convocare Consigli - Giunte – Assemblee; per gestire le comunicazioni ufficiali; per **notificati atti legali**, contratti, diffide, richieste, se firmati digitalmente; per la trasmissione di documentazione relativa ai **rapporti tra Ente e dipendenti.**

9.6 L'indirizzo di PEC assegnata al Protocollo Generale del Comune di Ariano Irpino è: ***protocollo.arianoirpino@asmepec.it***

10. Uso della rete Internet e dei relativi servizi

10.1 Il Personal Computer assegnato al dipendente ed abilitato alla navigazione in Internet costituisce uno strumento necessario utilizzabile esclusivamente allo svolgimento della propria attività lavorativa. E' assolutamente proibita la navigazione in Internet per motivi diversi da quelli legati all'attività lavorativa stessa. **Sono pertanto vietati**:

- l'uso di Internet per lo scarico di file del tipo MP3, AVI, MPG, Quicktime, e/o altri tipi di files o programmi freeware/shareware non legati ad un uso d'ufficio, se non espressamente autorizzato dal Responsabile S.I.C.;

- l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dal Dirigente di Area o dal Responsabile del Servizio congiuntamente al Responsabile S.I.C. attinenti i compiti e le mansioni assegnate e con il rispetto delle normali procedure di acquisto;

- la registrazione, l'uso e la navigazione su siti non legati ad esigenze esclusivamente di tipo lavorativo. A tal fine il Responsabile S.I.C. provvede ad inibire la consultazione dei siti web non utili alla produttività dell'Ente e, soprattutto, potenzialmente lesivi per l'infrastruttura con l'adozione di uno specifico sistema di blocco o filtro automatico (firewall) che impedirà determinate operazioni quali l'upload o l'accesso a determinati siti inseriti in una black list;

- la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames), se non attinenti l'attività lavorativa svolta;

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

- l'accesso alla rete internet in orari differenti da quello di lavoro. A tal fine il responsabile della sicurezza informatica, d'accordo con i responsabili di servizio, indicherà un orario di massima per la

concessione del servizio di accesso ad internet. Il S.I.C. si riserva di applicare per singoli e gruppi di utenti politiche di navigazione personalizzate in base alle mansioni ed eventuali disposizioni concordate con l'Amministrazione e con i Dirigenti di Area o Responsabili di Servizio, al fine di ottimizzare l'uso delle risorse, gli investimenti e le prestazioni delle connessioni esistenti;

- l'utilizzo di qualsiasi mezzo alternativo (router, modem o altro) al collegamento Lan dell'Ente per connettersi ad Internet;

- l'accesso alla rete dall'esterno via modem o con qualsiasi altro mezzo di accesso remoto senza l'autorizzazione del Responsabile S.I.C.;

- lo svolgimento di qualsiasi attività intesa ad eludere o ingannare i sistemi di controllo di accesso e/o sicurezza di qualsiasi server interno o pubblico, incluso il possesso o l'uso di strumenti o software intesi ad eludere schemi di protezione da copia abusiva del software, rivelare password, identificare eventuali vulnerabilità della sicurezza dei vari sistemi, decrittare file crittografati o compromettere la sicurezza della rete e internet in qualsiasi modo;

- Ai soli fini di gestione e di salvaguardia degli interessi dell'Ente e dei propri dipendenti, l'Amministrazione adotta misure di filtraggio mediante un sistema di controllo dei contenuti (Firewall, Proxy server, ecc…) o mediante "file di log" della navigazione svolta. Il controllo sui file di log non è continuativo ed i file stessi vengono conservati non oltre 6 mesi, in analogia a quanto previsto nel provvedimento
del 24.7.2008 del Garante per la protezione di dati personali.

11. Protezione antivirus

11.1 Il sistema informatico del Comune di Ariano Irpino è protetto da software antivirus aggiornato quotidianamente attraverso filtro automatico (firewall). Ogni utente deve tenere comportamenti tali da proteggere i dati personali contro il rischio di intrusione e dall'azione di programmi di cui all'art. 615-quinquies del Codice Penale, aventi per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione totale o parziale, o l'alterazione del suo funzionamento.

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

11.3 Nel caso che il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer e segnalare prontamente l'accaduto al personale S.I.C.;

11.4 Non è consentito l'utilizzo di hard disk esterni, penne USB, floppy disk, cd rom, cd riscrivibili, nastri magnetici di provenienza ignota.

11.5 Ogni dispositivo magnetico di provenienza esterna dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato al personale S.I.C..

12. Utilizzo dei telefoni, fax e fotocopiatrici dell'Ente

12.1 Il telefono eventualmente affidato all'utente è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, non essendo quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti l'attività lavorativa stessa. La ricezione o l'effettuazione di telefonate personali è consentito solo nel caso di comprovata necessità ed urgenza.

12.2 Qualora venisse assegnato un cellulare aziendale al dipendente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Al cellulare si applicano le medesime regole sopra previste per l'utilizzo del telefono aziendale: in particolare è vietato l'utilizzo del telefono cellulare messo a disposizione per inviare o ricevere SMS o MMS di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa. L'eventuale uso promiscuo (anche per fini personali) del telefono cellulare è possibile soltanto in presenza di preventiva autorizzazione scritta e in conformità delle istruzioni al riguardo impartite dal Segretario Generale.

12.3 È vietato l'utilizzo dei fax per fini personali, tanto per spedire quanto per ricevere documentazione, salva diversa esplicita autorizzazione da parte del Dirigente dell' Area o del Responsabile del Servizio.

12.4 È vietato l'utilizzo delle fotocopiatrici per fini personali, salvo preventiva ed esplicita autorizzazione da parte del Dirigente dell' Area o del Responsabile del Servizio.

13. Utilizzo di supporti cartacei

13.1 Gli incaricati del trattamento devono prelevare dagli archivi i soli atti e documenti loro affidati, che devono controllare e custodire, durante l'intero ciclo necessario per lo svolgimento delle operazioni di trattamento, per poi restituirli all'archivio, al termine di tale ciclo.

13.2 Per gli atti ed i documenti contenenti dati sensibili, il controllo e la custodia devono avvenire in modo tale che ai dati non accedano persone prive di autorizzazione.

13.3 Per i documenti contenti dati sensibili, è necessario che l'incaricato del trattamento utilizzi cassetti con serratura, o altri accorgimenti aventi funzione equivalente, nei quali riporli prima di assentarsi dal posto di lavoro, anche se temporaneamente. In tali cassetti i documenti potranno essere riposti al termine della giornata di lavoro, qualora l'incaricato debba utilizzarli anche nei giorni successivi; al termine del trattamento l'incaricato dovrà invece restituirli all'archivio.

13.4 Agli archivi contenenti dati sensibili possono accedere sempre e comunque i soli soggetti autorizzati

13.5 Per gli accessi agli archivi contenenti dati sensibili che avvengono dopo l'orario di chiusura, è obbligatorio identificare e registrare coloro che vi accedono.

14. Acquisto di strumenti Informatici Hardware - Software e manutenzione

14.1 Ai fini della valutazione della congruità delle offerte e nell'ottica dell'ottimizzazione e risparmio delle risorse oltre ad una integrazione all'interno della rete Comunale, tutti gli atti riguardanti gli

acquisti di strumenti informatici e telematici (Hardware e Software), dovranno riportare il visto del Responsabile S.I.C., e preventivamente valutati con apposita relazione del personale S.I.C., per verificare se gli approvvigionamenti si ispirano a i principi di economicità, efficienza e funzionalità, perseguendo la standardizzazione sia del hardware che del software, nelle caratteristiche, marche, modelli, standard di qualità, ecc.

14.2 Le forniture di cui al punto 14.1 dovranno avvenire alla presenza di personale S.I.C. che valuterà la congruenza della fornitura all'ordine e trasmetterà all'economo comunale la documentazione inerente l'acquisto per l'inventariazione del bene specificando l'utente assegnatario della risorsa.

14.3 Il S.I.C. si occupa della manutenzione dell'Hardware e del software esistenti nell'Ente avvalendosi se necessario di fornitori esterni, coordinando i vari interventi e verificandone l'esatta applicazione, nel rispetto delle normative vigenti, ispirandosi a principi di economicità, efficienza e funzionalità. Eventuali richieste di manutenzione hardware e software devono essere comunicate attraverso e-mail al Responsabile S.I.C. specificando il problema e l'intervento.

15. Responsabilità e Osservanza delle disposizioni in materia di Privacy

15.1 Ogni utente è responsabile, civilmente e penalmente, del corretto uso delle risorse informatiche, con particolare riferimento ai servizi, ai programmi a cui ha accesso e ai dati trattati a fini istituzionali. E' altresì responsabile del contenuto delle comunicazioni effettuate e ricevute a fini istituzionali anche per quanto attiene la riservatezza dei dati ivi contenuti, la cui diffusione impropria potrebbe configurare violazione del segreto d'ufficio o della normativa per la tutela dei dati personali. Sono inoltre vietati comportamenti che possono creare un danno, anche di immagine, all'Ente.

15.2 È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza, come indicato nella lettera di designazione ad incaricato del trattamento dei dati ai sensi del Disciplinare tecnico allegato al D.Lgs. n. 196/2003.

15.3 Oltre che per motivi di sicurezza del sistema informatico, anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.) o per finalità di controllo e programmazione dei costi (ad esempio, verifica costi di connessione ad internet, traffico telefonico, etc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà della Amministrazione, tramite il personale S.I.C., accedere direttamente, nel rispetto di quanto stabilito dalla normativa sulla Privacy dal Garante e dello statuto dei lavoratori, a tutti gli strumenti informatici comunali e ai documenti ivi contenuti, nonché ai tabulati del traffico telematico.

16. Flusso documentale

16.1 L'informatizzazione del Comune di Ariano Irpino è estesa al trattamento dei documenti nell'ambito dei processi. Gli Uffici sono tenuti ad utilizzare le applicazioni informatiche predisposte all'iter documentale e all'interoperabilità tra i Servizi.

16.2 Oltre a gestire l'iter dei documenti, il sistema gestisce e controlla le attività del procedimento, non è consentito pertanto utilizzare software, se pur funzionali, isolati dal sistema applicativo integrato.

17. Sistemi di controlli graduali

17.1 L'Amministrazione si riserva di effettuare controlli sul corretto utilizzo degli strumenti informatici, della posta elettronica, di internet, nel rispetto delle normative vigenti e del presente regolamento.

17.2 Per motivi di sicurezza e protezione dei dati, ogni attività compiuta nella rete Informatica può essere sottoposta a registrazione in appositi file di log e riconducibili, indirettamente, all'utente. Detti file possono essere soggetti a trattamento solo per fini istituzionali, per attività di monitoraggio e controllo e possono essere messi a disposizione dell'Autorità Giudiziaria in caso di accertata violazione delle norme vigenti. La riservatezza delle informazioni è soggetta a quanto dettato dal D. Lgs. 196/2003 e s.m.i. e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori.

17.3 In caso di anomalie, il personale incaricato del S.I.C. effettuerà controlli anonimi che si concluderanno con avvisi generalizzati diretti ai dipendenti del settore in cui è stata rilevata l'anomalia, si evidenzierà l'utilizzo irregolare degli strumenti informatici e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

17.4 Nel caso in cui si riscontrino ulteriori anomalie e dati di carattere personale, inerenti le attrezzature informatiche assegnate ai singoli dipendenti, potranno essere attuati controlli su base individuale, assicurando di fornire preventivamente una adeguata informativa, non entrando nel merito dei contenuti ed esplicitando le motivazioni che rendano necessario tale controllo e la modalità con cui sarà effettuato.

17.5 In alcun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

18. Formazione e Aggiornamento

18.1 Il Comune di Ariano Irpino promuove, all'interno del piano annuale della formazione, l'aggiornamento e la formazione dei propri dipendenti in merito al corretto utilizzo delle strumentazioni informatiche.

19. Sanzioni

19.1 È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente regolamento. Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile nei confronti del personale dipendente con provvedimenti disciplinari e risarcitori previsti dalla vigente normativa, nonché con tutte le azioni civili e penali consentite.

20. Aggiornamento e revisione

20.1 Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Le proposte verranno esaminate dal S.I.C., istruite e sottoposte al Responsabile del S.I.C. per la trasmissione al Consiglio Comunale.

21. Entrata in vigore del Regolamento e Pubblicità

21.1 Con l'entrata in vigore del presente Regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi sostituite dalle presenti.

21.2 Copia del presente regolamento verrà consegnata a ciascun Dirigente di Area e/o Responsabile di Servizio, affinché rendano noti i contenuti ai rispettivi incaricati, nonché affisso in modo permanente in luogo visibile a tutti i dipendenti e pubblicato sul sito internet del Comune.

21.2 Il presente regolamento è consegnato agli utenti interni di cui al comma 1.1, che lo sottoscrivono per presa visione e accettazione, quale parte integrante del contratto di lavoro o altra forma di collaborazione, (cfr. art. 23).

21.3 Per quanto non previsto o contemplato nel presente Regolamento si rimanda ai riferimenti normativi in calce.

22. Elenco dei Responsabili della Privacy e loro mansioni

22.1

Settore	Responsabile del Trattamento
Segretario Generale	
Area Amministrativa	
Area Tecnica	
Area Finanziaria	
Area Vigilanza	

23. Presa visione ed accettazione del regolamento

Presa visione ed accettazione del regolamento

Il sottoscritto/a _____
Nato/a _____
Residente _____ in via_____
Telefono _____ cod. fisc. _____

Dichiara di:

- aver preso visione ed accettare tutte le norme contenute nel regolamento d'uso del sistema Informativo del Comune di Ariano Irpino (AV).
- aver acquisito le informazioni di cui all'art. 13 del Decreto Legislativo 196 del 30 Giugno 2003;
- essere a conoscenza dei diritti dell'interessato di cui agli articoli 7, 8, 9, 10, del medesimo decreto.

Data _____ Firma _____

Riferimenti Normativi:

Garante della Privacy D.Lgs 196/03 e s.m.i.,"Linee Guida per posta elettronica e internet" del 1 marzo 2007"

Garante della Privacy D.Lgs 196/03 e s.m.i.," Misure ed accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di Sistema" del 27 novembre 2008"

Codice dell'Amministrazione Digitale D. Lgs. n. 82/2005) e s.m.i.

Artt. 76, 87, 117 della Costituzione; L. 7 agosto 1990, n.241, Direttiva 1999/93 CE, DPR 28 dicembre 2000, n. 445; D. Lgs 30 giugno 2003, n. 196; L. 9 gennaio 2004, n. 4; Deliberazione CNIPA 19 febbraio 2004, n. 11; L. 15 del 2005; D. Lgs 7 marzo 2005, n.82 (*Codice dell'Amministrazione Digitale*) e successive modificazioni ed integrazioni;

Dlg. 518/92 sulla tutela giuridica del software e L. 248/2000 nuove norme di tutela del diritto d'autore;

DPR 11 febbraio 2005, n. 68 "Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3." (G.U. 28 aprile 2005, n. 97);
Decreto Ministeriale 2 novembre 2005 "Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata" (G.U. del 14 novembre 2005, n. 265);
Decreto Legislativo 7 marzo 2005, n. 82 "Codice dell'amministrazione digitale " (G.U. 16 m aggio 2005, n. 93), integrato dal D.lgs. n.159/2006;

D.lgs n. 150/2009 - Ottimizzazione della produttività del lavoro pubblico, efficienza e trasparenza delle PA;

Circolare n. 1/2010/DDI della Presidenza del Consiglio dei Ministri "Uso della Posta Elettronica Certificata nelle Amministrazioni Pubbliche";

Circolare n. 2/2010/DDI della Presidenza del Consiglio dei Ministri "Informazioni per la gestione delle caselle di **PEC**";

Codice disciplinare pubblicato dal Comune di Ariano Irpino (AV) dei dirigenti e dipendenti del comparto Regioni Enti Locali ai sensi dell'art. 55, comma 2, del D.Lgs 165/2001.