CITTÀ DI AGROPOLI

(Provincia di Salerno)

DELIBERAZIONE DELLA GIUNTA COMUNALE

copia **n°. 32 del 27/01/2011**

OGGETTO : APPROVAZIONE DEL "REGOLAMENTO DI ORGANIZZAZIONE DEI CRITERI E MODALITA' OPERATIVE PER L'UTILIZZO DELLE APPARECCHIATURE INFORMATICHE"

L'anno duemilaundici il giorno ventisette del mese di gennaio alle ore 12,40 nella Casa Comunale, regolarmente convocata si è riunita la Giunta Comunale, composta da:

Avv.	Francesco Alfieri	Sindaco
Ing.	Mauro Inverso	Vice Sindaco
Dott.	Antonio Pepe	Assessore
Sig.	Franco Crispino	Assessore
Sig.	Angelo Coccaro	Assessore
Ing.	Raffaele Carbone	Assessore
Dott.	Adamo Coppola	Assessore
Avv.	Eugenio Benevento	Assessore

Risultano assenti : / /.

Assume la presidenza il Sindaco Avv. Francesco Alfieri

Partecipa il Segretario Generale dott.ssa Angela Del Baglivo.

Proponente: Responsabile del Servizio informatizzazione ed innovazione tecnologica

Oggetto : Approvazione del "Regolamento di organizzazione dei criteri e modalità operative per l'utilizzo delle apparecchiature informatiche"

PREMESSO
Che il D. Lgs. 30/06/2003 n.196 e successive modifiche ed integrazioni "Codice in materia di protezione dei dati personali", impone anche alle Pubbliche Amministrazioni titolari del trattamento dei dati personali, l'adozione di "misure minime di sicurezza", volte ad evitare -con idonee misure organizzative, logistiche e procedurali- i rischi connessi al trattamento con strumenti elettronici dei dati personali, sensibili e giudiziari, detenuti per finalità connesse al perseguimento degli scopi istituzionali;
che oltre a realizzare gli interventi necessari a garantire la sicurezza dei dispositivi informatici e delle procedure di salvataggio, conservazione e ripristino dei dati; è altresì necessario disciplinare con apposito regolamento i criteri e le modalità operative per l'utilizzo delle apparecchiature informatiche e per l'accesso e utilizzo del servizio internet e di posta elettronica da parte dei dipendenti del Comune e di tutti gli altri soggetti che a vario titolo prestano servizio o attività per conto e nelle strutture del Comune di Agropoli (lavoratori socialmente utili, collaboratori, tirocinanti/stagisti).

RITENUTO
di dover approvare la proposta predisposta dal responsabile del Servizio informatizzazione ed innovazione tecnologica e di adottare il "Regolamento di organizzazione dei criteri e modalità operative per l'utilizzo delle apparecchiature informatiche"

DATO ATTO
che l'adozione della presente delibera non comporta aumento di spesa per l'Ente;

VISTI
il Dlgs 30 marzo 2001, n. 165 e successive modifiche ed integrazioni
il D. Lgs. 30/06/2003 n.196 e successive modifiche ed integrazioni
il DL 25/6/2008, n. 112 convertito, con modificazioni, in legge 6/8/2008, n. 133

Per tutto quanto esposto in premessa,

PROPONE DI DELIBERARE

1. approvare il "Regolamento di organizzazione dei criteri e modalità operative per l'utilizzo delle apparecchiature informatiche" allegato sub "A" alla presente delibera, di cui forma parte integrante e sostanziale.
2. Trasmetterne copia ai Responsabili degli Uffici e dei Servizi comunali che provvederanno a portarlo a conoscenza del personale assegnato all'Area di competenza, e ne cureranno l'osservanza.
3. Dare informazione alle OO.SS. dei dipendenti dell'Approvazione del presente Regolamento.

Agropoli,lì 15 dicembre 2010

Firma del proponente
Il Responsabile del Servizio
informatizzazione ed innovazione tecnologica
f.to Giuseppe Salurso

PARERE TECNICO : Responsabile del Servizio informatizzazione ed innovazione tecnologica
- Vista la proposta di cui sopra, ai sensi dell'art. 49 comma 1 del TU delle leggi sull'ordinamento degli EELL, approvato con D.Lgs 18/08/2000, n°267; per quanto riguarda la sola regolarità tecnica,esprime parere favorevole.

Data 15 dicembre 2010

Il Responsabile del servizio
f.to Giuseppe Salurso

COMUNE DI AGROPOLI

Regolamento di organizzazione dei criteri e modalità operative per l'utilizzo delle apparecchiature informatiche

Adottato con deliberazione della Giunta Municipale n. ____ del _____

SOMMARIO

COMUNE DI AGROPOLI

Regolamento di organizzazione dei criteri e modalità operative per l'utilizzo delle apparecchiature informatiche

1. PREMESSA

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

L'utilizzo delle risorse informatiche e telematiche dell'Ente deve sempre ispirarsi al principio della diligenza e correttezza dei comportamenti cui tutti sono obbligati nell'ambito del rapporto di lavoro.

Il presente regolamento è finalizzato ad evitare che taluni comportamenti (siano essi volontari o inconsapevoli) possano creare problemi o minacce alla sicurezza nel trattamento dei dati.

Tali prescrizioni si aggiungono ed integrano le specifiche istruzioni che vanno fornite dai responsabili dei servizi e dall' Amministratore di Sistema a tutti gli incaricati in attuazione del D.lgs 196/03 "Testo Unico in materia di protezione dei dati personali".

2. DEFINIZIONI

1. **AdS**: Amministratore di Sistema.
2. **BLACK LIST**: elenco di siti non accessibili da nessun utente.
3. **ID UTENTE** o **USER ID:** identifica l'utente di una rete, di un servizio telematico o di un sito Internet. Di norma viene utilizzato accoppiato con una password.
4. **INTERNET PROVIDER:** azienda che fornisce il canale di accesso alla rete internet.
5. **LOG**: archivio delle attività di consultazione in rete.
6. **PASSWORD:** sequenza di lettere e numeri che permette di identificare un utente specifico. digitando correttamente questi caratteri si può avere accesso al computer o alla rete.
7. **POSTAZIONE DI LAVORO:** personal computer collegato alla rete comunale tramite il quale l'utente accede ai servizi.
8. **RSI**: Responsabile del Sistema Informativo Comunale.
9. **UTENTE DI POSTA ELETTRONICA**: persona autorizzata ad accedere al servizio di posta elettronica.
10. **UTENTE INTERNET** (**AMPIO**): persona autorizzata ad accedere al servizio internet al di là dei siti istituzionali preventivamente selezionati dal Comune, con l'unico limite di filtri predeterminati che si attivano in modo automatico durante la navigazione.
11. **UTENTE INTERNET** (**BASE**): persona autorizzata ad accedere alla lista di siti istituzionali preventivamente selezionati.
12. **WHITE LIST**: elenco di siti direttamente e immediatamente accessibili da tutti gli utenti internet (base).

3. MODALITÀ DI ACCESSO E DI UTILIZZO DEI SERVIZI INFORMATICI

Per accedere ai servizi informatici da una postazione di lavoro l'utente deve utilizzare un codice identificativo (id utente) e una parola chiave segreta (password). Superato il sistema di autenticazione l'utente è collegato alla rete aziendale e ad internet senza ulteriori formalità.

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

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

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

L'utente può essere chiamato a rispondere, oltre che per i propri fatti illeciti, anche per quelli commessi da chiunque utilizzi il suo codice identificativo e/o password.

La violazione delle presenti disposizioni può comportare l'applicazione delle sanzioni disciplinari previste dal vigente CCNL, rimanendo ferma ogni ulteriore forma di responsabilità civile e penale.

- **GESTIONE DELLE PASSWORD**

La conoscenza della password da parte di terzi consente agli stessi l'accesso alla rete aziendale, l'utilizzo dei relativi servizi in nome dell'utente titolare e l'accesso ai dati cui il medesimo è abilitato, con la possibilità di visualizzazione di informazioni riservate, distruzione o modifica dei dati, lettura della posta elettronica, uso indebito di servizi ecc.

Di qualsiasi azione o attività svolta utilizzando il codice identificativo e/o la password assegnata è responsabile l'utente assegnatario del codice; pertanto ogni utente, deve:

13. Conservare le password con la massima riservatezza e diligenza. La password deve rispondere alle specifiche previste dall'allegato B del D.lgs 196/2003, ovvero deve essere di tipo alfanumerico, lunghezza minima di 8 caratteri e non ripetibile almeno una volta. Il Responsabile del Sistema Informativo del Comune e/o l'Amministratore di Sistema provvederà ad impostare l'obbligatorietà della password e a settare il sistema secondo le specifiche di legge.
14. Ogni utente dovrà consegnare, in busta chiusa, al "Custode delle password" indicato dal responsabile della propria Area: la password di accesso al Sistema Operativo del proprio PC,

l'eventuale password di BIOS (obbligatoria sui sistemi operativi Windows 95/98), l'eventuale password di rete, di accesso al database in uso presso la postazione in oggetto e di posta elettronica, nonché tutti gli "User Id" e le password per l'accesso ad eventuali servizi online a cui abbia accesso.

15. Non attivare password d'accensione (bios), senza preventiva autorizzazione.
16. Non utilizzare credenziali (user-id e password) di altri utenti, nemmeno se fornite volontariamente o di cui si ha casualmente conoscenza.
17. Ove più di un utente acceda alla stessa postazione, occorrerà prevedere un account per ogni singolo operatore e dotare l'account di password secondo le specifiche di cui sopra.

- **POSTAZIONE DI LAVORO**

Ogni utente è responsabile della postazione assegnatagli e del contenuto del relativo disco fisso. Pertanto l'utente, deve mantenere la corretta configurazione del proprio computer non alterando le componenti hardware e software predisposte allo scopo.
É vietato perciò installare programmi diversi da quelli autorizzati dal Sistema Informativo Aziendale per evitare di rendere instabile il sistema operativo e mettere a rischio la sicurezza del PC e del sistema informativo, l'integrità dei dati e la loro ripristinabilità oppure favorirne la diffusione accidentale.

Ogni utente deve inoltre adottare le seguenti precauzioni:

18. Non lasciare incustodita ed accessibile la propria postazione una volta connesso al sistema con le proprie credenziali di autenticazione.
19. Non cedere l'uso della propria postazione a personale non autorizzato, in particolar modo per quanto riguarda l'accesso a internet e ai servizi di posta elettronica.
20. Spegnere il Personal Computer al termine dell'orario di lavoro o in caso di assenze prolungate dall'ufficio.
21. Impostare lo "screensaver" con password al fine di non lasciare a vista la postazione in caso di allontanamento temporaneo.
22. Evitare di inserire supporti magnetici di qualsiasi tipo (es. floppy disk, CD, DVD, Pen drive, Schede di memoria ecc.) di provenienza dubbia o ignota (es. allegati a riviste acquistate in edicola).
23. Non riprodurre o duplicare programmi informatici (ai sensi delle Legge n.128 del 21/5/2004).
24. Evitare di collegare all'impianto di alimentazione dedicato al funzionamento dei computer apparecchiature elettriche diverse da quelle installate e/o autorizzate dall'AdS o dall'RSI. (stufette, condizionatori, fax, fotocopiatrici ecc.)

- **SICUREZZA DEI DATI**

Ogni utente deve tenere comportamenti tali da garantire la sicurezza dei dati contenuti nel sistema informativo dell'Ente e ridurre i rischi di perdita, danneggiamento o diffusione non autorizzata degli stessi. Pertanto l'utente, deve:

25. Utilizzare regolarmente di un sistema di backup automatizzato dei dati da effettuarsi su supporto esterno da conservare in cassaforte di area o comunque in luogo sicuro ed inaccessibile a terzi.
26. Archiviare informaticamente esclusivamente le informazioni previste dalla legge o necessarie all'attività lavorativa.
27. Evitare di scaricare o salvare file non istituzionali di qualsiasi tipo (es: file audio o video) nelle connessioni di rete su cui viene eseguito il back-up dei dati.
28. È assolutamente vietato permettere a persone diverse da quelle di volta in volta indicate effettuare condivisioni di rete o modificare il settaggio delle stesse.
29. Nel caso in cui il PC è collegato ad un server e una rete LAN con Dominio, il backup dei dati dovrà essere automatizzato direttamente da Server. Ogni utente deve dotarsi di un registro di backup su cui annotare le operazioni. Mensilmente va effettuata, insieme all'RSI comunale, una prova di ripristino backup.

- **PROTEZIONE ANTIVIRUS**

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

30. Ogni utente è tenuto a controllare la presenza e il regolare funzionamento del software antivirus. È illegale l'utilizzo di software freeware per solo uso personaleper i quali è necessaria una licenza d'uso per utilizzo in ambito aziendale.
31. Ogni dispositivo magnetico di provenienza esterna all'Ente dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus non eliminabile

dal software, non dovrà essere utilizzato.

32. Nel caso che il software antivirus rilevi la presenza di un virus che non è riuscito a ripulire, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer e segnalare l'accaduto al responsabile per la sicurezza

4. UTILIZZO DI PC PORTATILI

L'utente è responsabile del PC portatile eventualmente assegnatogli e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro. Ai PC portatili si applicano le regole di utilizzo previste per i Pc connessi in rete con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.

33. I PC portatili utilizzati all'esterno (convegni, stage, sopralluoghi), in caso di allontanamento, devono essere custoditi in un luogo protetto.
34. Il portatile non deve essere mai lasciato incustodito e sul disco devono essere conservati solo i file strettamente necessari.
35. Nel caso di accesso alla rete aziendale tramite Accesso Remoto utilizzare l'accesso in forma esclusivamente personale utilizzare la password in modo rigoroso.
36. Disconnettersi dal sistema di Accesso Remoto al termine della sessione di lavoro.
37. Collegarsi periodicamente alla rete interna per consentire il caricamento dell'aggiornamento dell'antivirus.
38. Non utilizzare abbonamenti Internet privati per collegamenti alla rete.

5. GESTIONE DEGLI ACCESSI IN RETE E CONDIVISIONE RISORSE

la gestione dei Gruppi di lavoro e degli IP di rete e dei DNS deve essere effettuata esclusivamente all'RSI e/o all'AdS. Una volta che l'RSI o l'AdS ha stabilito l'IP, i DNS e il gruppo di lavoro per una specifica postazione, è vietato modificare, anche solo parzialmente, le impostazioni di rete.

39. L'assegnazione di indirizzi IP, in caso di installazione di una qualsiasi periferica di rete (stampante, fax, HD ecc), va effettuata esclusivamente dall'RSI o dall'AdS.
40. Ogni condivisione dei dischi fissi o altre periferiche (stampanti, fax, etc) deve essere richiesta dal Responsabile dell'Area al RSI o all'AdS che provvederà solo dopo aver verificato che la connessione non pregiudichi l'integrità, la non alterabilità, e la sicurezza dei dati e criteri opportuni di accesso alle risorse.
41. Gli operatori del Sistema Informativo possono in qualunque momento procedere alla rimozione di ogni file o applicazione che riterranno essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.
42. L'installazione di software o la modifica della sua configurazione; la configurazione dei servizi di accesso ad internet e di posta elettronica deve essere eseguita esclusivamente da personale incaricato dal Comune.

6. INTERNET

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

L'utilizzo ampio di internet, non limitato cioè alla lista di siti individuata come sopra, è autorizzato per i responsabili delle strutture. Gli stessi, in caso di esigenze particolari adeguatamente motivate, possono richiedere per altri dipendenti l'autorizzazione all'accesso a siti non inseriti nella withe list.

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

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

È in ogni caso sempre vietato l'accesso a siti ove è possibile scaricare software, pubblicazioni, musica, film o altro materiale protetto da diritto d'autore; accedere a siti o a richieste di prestazioni e servizi a pagamento (es. giochi o scommesse online, acquisti on line); accedere a siti che richiedano di installare programmi o applicazioni; accedere a siti aventi contenuti contrari all'ordine pubblico o al buon costume (es. contenenti materiale pedo-pornografico, che incitino all'odio razziale ecc.); oppure nei siti contenuti in un'apposita lista che sarà divulgata dall'Amministrazione comunale (BLACK LIST).

L'utente è direttamente responsabile dell'uso del servizio di accesso a internet, dei contenuti che vi

ricerca, dei siti che contatta, delle informazioni che vi immette e delle modalità con cui opera.

All'utente non è consentito:

43. utilizzare internet provider diversi da quello ufficiale del Comune e la connessione di stazioni di lavoro aziendali alle reti di tali provider con sistemi di connessione diversi da quello centralizzato;
44. servirsi o dar modo ad altri di servirsi della stazione di accesso a internet per attività non istituzionali, per attività poste in essere in violazione del diritto d'autore o altri diritti tutelati dalla normativa vigente;
45. utilizzare sistemi Peer to Peer (P2P), di file sharing, podcasting, webcasting o simili, così come connettersi a siti che trasmettono programmi in streaming (come radio o TV via WEB), o programmi di chat (IRC, MIRC ecc.) senza previa autorizzazione del Responsabile del sistema informativo;
46. scaricare software prelevato da siti Internet, se non espressamente autorizzato dal Responsabile del Servizio Sistemi Informativi;
47. effettuare transazioni finanziarie, operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati o attinenti i compiti e le mansioni assegnate e con il rispetto delle normali procedure di acquisto;
48. ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;
49. 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;
50. usare la rete in modo difforme da quanto previsto dal presente documento e dalle leggi penali, civili e amministrative in materia di disciplina dell'attività e dei servizi svolti sulla rete.

7. POSTA ELETTRONICA

L'utilizzo del servizio di posta elettronica è consentito solo per ragioni di servizio agli utenti identificati con le modalità precedentemente illustrate, ai quali il Comune assegna una casella di posta personale e nominativa.
La casella del Servizio/Ufficio è accessibile solo in modalità di delega, previa richiesta e autorizzazione del Responsabile della struttura.
In caso di assenza, l'utente può delegare altro dipendente dell'ufficio a verificare il contenuto dei messaggi e ad inoltrare al Responsabile del sistema informativo quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa.

All'utente non è consentito:

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

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

8. MONITORAGGIO E CONTROLLI

Il Comune può avvalersi di sistemi di controllo del corretto utilizzo degli strumenti di lavoro che consentono indirettamente un controllo a distanza dell'effettivo adempimento della prestazione lavorativa e determinano un trattamento di dati personali riferiti o riferibili ai lavoratore nel rispetto di quanto previsto dal Provvedimento del garante della Privacy 1/3/2007 n. 13.

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

Le attività sull'uso del servizio di accesso ad internet possono essere automaticamente registrate in forma elettronica attraverso i "LOG" di sistema. Il trattamento dei dati contenuti nei LOG può avvenire esclusivamente in forma anonima in modo tale da precludere l'identificazione degli utenti

e/o delle loro attività.

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

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

I dati personali contenuti nei log possono essere trattati nelle seguenti ipotesi:

56. per corrispondere ad eventuali richieste della polizia postale e/o dell'autorità giudiziaria;
57. su richiesta del Responsabile del sistema informativo quando si verifichi un evento dannoso o una situazione di pericolo che richieda un immediato intervento;
58. su richiesta del Responsabile del sistema informativo limitatamente al caso di utilizzo anomalo degli strumenti da parte degli utenti di una specifica struttura/area (rilevabile ad es. dal LOG) e reiterato nonostante l'invito agli utenti da parte del Responsabile del sistema informativo ad attenersi ai compiti assegnati ed alle istruzioni impartite.

I dati contenuti nei LOG sono conservati per il tempo strettamente necessario al perseguimento di finalità organizzative, produttive e di sicurezza, comunque non superiore a sei mesi, e sono periodicamente cancellati dal sistema.
I dati riguardanti il software installato sulle postazioni di lavoro possono essere trattati per finalità di verifica della sicurezza dei sistemi ed il controllo del rispetto delle licenze regolarmente acquistate.

9. REVOCA DEL SERVIZIO DI ACCESSO AD INTERNET

L'utilizzo del servizio di accesso ad internet può essere revocato nei seguenti casi:

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

10. SERVIZIO DI MANUTENZIONE ED ASSISTENZA HARDWARE E SOFTWARE

In caso di ricorso a tecnici esterni per cause di manutenzione ed assistenza software, occorre seguire le seguenti direttive:

67. Ogni volta che si renda necessario un intervento tecnico, su una apparecchiatura informatica (PC stampanti monitor ecc) responsabile di Area deve preventivamente informarne l'RSI.
68. Ogni PC del Comune è dotato di un "account Amministratore" protetto da password; il responsabile dell'Area, prima di consegnare la macchina al manutentore dovrà informare l'RSI o l'AdS che inserirà una password provvisoria comunicandola al manutentore. All'atto della riconsegna del PC, il responsabile dell'Area deve informare l'RSI o l'AdS che rimuoverà la password di accesso provvisoria.
69. In caso di intervento tecnico su di un PC che tratta dati, il tecnico manutentore diventa "un incaricato al trattamento dati" e pertanto deve essere autorizzato dal responsabile di Area in forma scritta. Nel caso in cui l'intervento debba effettuarsi al di fuori della casa comunale, se tecnicamente possibile, tutti i dati dovranno essere copiati su un diverso supporto e rimossi dal disco rigido prima della consegna. All'atto della consegna del PC l'incaricato dovrà assicurarsi dell'identità dell'interessato o di chi è stato delegato al ritiro del PC, annotando in una apposita scheda: la ditta esecutrice del lavoro, nominativo dell'addetto che effettua l'intervento o

provvede al ritiro della macchina, natura dell'intervento richiesto data e ora dell'intervento o del ritiro.

70. Nel caso di sostituzione hard disk contenenti dati personali, sensibili o giudiziari, gli hard disk stessi dovranno essere riconsegnati al Responsabile di Area il quale provvederà alla sua custodia o distruzione previo intervento dell'RSI. In ogni caso, l'hard disk sostituito va riconsegnato all'RSI del Comune.
71. In caso di backup di hard disk contenti dati personali, sensibili o giudiziari, il manutentore dovrà garantire l'integrità e completezza dei dati preesistenti e che nessun dato resti su hard disk di proprietà della Società manutentrice utilizzati per il travaso dei dati stessi.
72. In caso di manutenzione hardware, l'incaricato non è autorizzato ad accedere ai software applicativi installati sul PC stesso né può accedere a documentazione memorizzata nel disco fisso del PC stesso, tranne nel caso di richiesta di backup dei dati o di travaso dati da un disco ad un altro. In tal caso è sempre necessaria l'autorizzazione scritta da parte del Responsabile Area che affida il proprio PC alla ditta manutentrice hardware.
73. Il manutentore non dovrà installare alcun software (salvo specifica richiesta del responsabile area) e in tal caso dovrà essere dotato di regolare licenza d'uso. Non dovranno essere installati software non inerenti alla risoluzione del problema posto o che mettano a rischio l'integrità e la sicurezza dei dati. Tutti, i sistemi di protezione preesistenti i ed i parametri di rete non dovranno essere modificati.
74. In caso di fornitura di un nuovo PC, va consegnata al Responsabile di Area anche la regolare licenza d'uso del Sistema operativo e dei software applicativi installati, unitamente alla fattura. Sarà poi compito del Responsabile di Area consegnare all'RSI le licenze d'uso acquisite.
75. La ditta manutentrice hardware, all'atto della riconsegna del PC, fornirà al responsabile di Area una scheda su cui siano indicati dettagliatamente gli interventi effettuati. Tale scheda dovrà essere conservata e messa a disposizione a richiesta dell'Ads, dell'RSI o del Titolare del trattamento dati

La ditta manutentrice deve impegnarsi a:

76. Provvedere a misure di sicurezza fisica e logica tecnicamente in grado di precludere ogni danno al PC e quindi, indirettamente, al titolare del trattamento dati o a terzi.
77. Distruggere tutti i dati eventualmente in suo possesso una volta terminato l'intervento o conservarli esclusivamente, in conformità alla legge, per il tempo strettamente necessario.
78. Garantire il rispetto delle precedenti norme da parte del proprio personale.

La Giunta comunale

Vista la suesposta proposta di deliberazione;
Dato atto che su tale proposta di deliberazione è stato acquisito il parere favorevole, del Responsabile del Servizio, in ordine alla sola regolarità tecnica, ai sensi dell'art.49, I comma, del D.lgs n.267/2000;
Dato atto che con nota prot. 37108 del 16/12/2010 è stata data comunicazione preventiva alle OO.SS. e non è pervenuta nessuna richiesta di concertazione;
Ad unanimità di voti legalmente resi ed accertati

DELIBERA

Di approvare la proposta di deliberazione innanzi trascritta il cui testo si intende qui integralmente riportato.

Con separata votazione, a voti unanimi, la presente deliberazione è dichiarata immediatamente esecutiva ai sensi dell'articolo 134, comma 4, del decreto legislativo 18 agosto 2000, n. 267

letto, confermato e sottoscritto.

IL SINDACO
f.to Avv. Francesco Alfieri

L'ASSESSORE ANZIANO
f.to sig. ing. Mauro Inverso

IL SEGRETARIO GENERALE
f.to dott.ssa Angela Del Baglivo

Copia della presente deliberazione è stata pubblicata,in data odierna, all'Albo Pretorio on line di questo Comune.

Agropoli, li _03/02/2011

IL MESSO COMUNALE

f.to M.Barone

CERTIFICATO DI PUBBLICAZIONE

Si certifica, giusta relazione del Messo Comunale, che copia della presente deliberazione è stata pubblicata, in data odierna, all'Albo Pretorio on line di questo Comune per la prescritta pubblicazione di quindici giorni consecutivi.

Agropoli, li 03/02/2011

Il Dirigente
F.to Dott. Eraldo Romanelli