ASP

SERVIZIO SANITARIO REGIONALE
BASILICATA
Azienda Sanitaria Locale di Potenza

DELIBERAZIONE DEL DIRETTORE GENERALE

NUMERO 570 DEL 28 MAG. 2010

IMMEDIATAMENTE ESEGUIBILE

TRASMESSA A:

○ Collegio Sindacale il 28 MAG. 2010 ○ Controllo preventivo regionale il

OGGETTO Adozione del "REGOLAMENTO AZIENDALE PER L'UTILIZZO DELLE RISORSE INFORMATICHE E TELEMATICHE".

DIREZIONE PROPONENTE UO Valutazione, Incarichi e PO / Referente Privacy ASP/2

Documenti integranti il provvedimento

1

Numero Allegati

RISERVATO ALL'UNITÀ OPERATIVA PROPONENTE (IMPUTAZIONE BUDGET)

Centro di responsabilità €

Centro di costo €

IL DIRIGENTE DELL'UNITÀ OPERATIVA

CERTIFICATO DI PUBBLICAZIONE

Si certifica che la presente è stata pubblicata all'Albo Pretorio dell'Azienda Sanitaria Locale di Potenza

in data 28 MAG. 2010 Ex art. 44 – L.R.n. 39/2001 e s.m.i. e che la stessa vi rimarrà affissa per 5 gg. consecutivi

Potenza, 28 MAG. 2010

DATA

IL FUNZIONARIO DELEGATO
Luigi Martorano

Premessi e **Richiamati:**

- la L n 300/1970 "Norme sulla tutela della libertà e dignità del lavoratori, della libertà sindacale e dell'attività sindacale nel luoghi di lavoro e norme sul collocamento" e, in particolare, l'art 4 , sulle modalità di controllo a distanza dell'attività lavorativa e l'art. 8, sui divieti di indagini relative alle opinioni del lavoratore;
- il D Lgs n 196/2003 " Codice in materia di protezione dei dati personali" e, in particolare, il disciplinare tecnico in materia di misure minime di sicurezza, allegato allo stesso Codice (Allegato B), che impone specifiche modalità tecniche, da adottare per il caso di trattamento con strumenti elettronici;
- la Deliberazione, n 13, del 01/03/2007, del Garante Privacy, avente ad oggetto "Lavoro: le linee guida del Garante per posta elettronica e internet", che detta la disciplina relativa alla navigazione in internet ed alla gestione della posta elettronica nei luoghi di lavoro;
- la Deliberazione, n 23, del 14/06/2007, del Garante Privacy, avente ad oggetto "Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico", che prevede, anche in tale settore, il pieno rispetto dei principi posti a generale protezione dei dati personali, sempre informati ai criteri di liceità, pertinenza e trasparenza, i quali offrono un'adeguata tutela ai lavoratori;
- la L n 48/2008 "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno", che prevede una serie di reati, cd informatici, che si configurano laddove l'attività illecita abbia, come oggetto o mezzo dello stesso, un sistema informatico o telematico;- la Deliberazione Aziendale n 303, del 26/03/2010, con la quale è stato approvato il Documento Programmatico per la Sicurezza, dell'Azienda Sanitaria di Potenza e relativo all'anno 2010;

Visti, in particolare, gli artt 2, 3 e 13 del D Lgs n 196/2003, con i quali, rispettivamente, si stabilisce che ogni attività relativa al trattamento di dati, ivi compresa, quindi, l'attività di controllo dettata da motivi di sicurezza, debba avvenire nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato; debba mostrarsi rispettosa dei principi fondamentali di necessità/ proporzionalità e debba essere pubblicizzata a mezzo di un'adeguata e preventiva informativa agli interessati;

Ritenuto utile adottare un apposito regolamento informatico intitolato "REGOLAMENTO AZIENDALE PER L'UTILIZZO DELLE RISORSE INFORMATICHE E TELEMATICHE", allegato alla presente e di cui costituisce parte integrante e sostanziale, che detti regole interne di condotta, dirette ad evitare comportamenti inconsapevoli e/o scorretti, in merito all'utilizzo delle risorse informatiche e telematiche aziendali, che, così come ogni altro comportamento posto in essere in ambito lavorativo, sempre devono ispirarsi al rispetto dei principi di diligenza e correttezza;

Considerato che, ex art 4, co 2, L n 300/1970, detto regolamento, anche al fine di scongiurare, a mezzo del sistema informatico, ogni forma di controllo a distanza sull'attività lavorativa, doveva adottarsi previo accordo con le Organizzazioni Sindacali, rappresentative del Comparto e della Dirigenza;

Rilevato che le Organizzazioni Sindacali rappresentative del personale aziendale del Comparto e della Dirigenza, negli incontri con la Delegazione trattante di parte pubblica, del 26.04.2010 e del 18.05.2010, come si evince dai rispettivi verbali di pari data, hanno espresso il proprio accordo in merito al contenuto del regolamento informatico aziendale, approvandolo in ogni suo punto;

con il parere favorevole del Direttore Amministrativo e del Direttore Sanitario,

DELIBERA

per tutto quanto in premessa espresso e richiamato,

- di adottare il regolamento informatico "REGOLAMENTO AZIENDALE PER L'UTILIZZO DELLE RISORSE INFORMATICHE E TELEMATICHE", allegato alla presente e di cui costituisce parte integrante e sostanziale, che stabilisce regole interne di condotta, dirette ad evitare comportamenti inconsapevoli e/o scorretti, in merito all'utilizzo delle risorse informatiche e telematiche aziendali;

• di informare, con adeguata comunicazione, tutti i responsabili del trattamento aziendali, dell'avvenuta pubblicazione del presente atto e del regolamento informatico su Intranet Aziendale, affinchè divulghino, con apposita informativa, in ogni struttura o reparto di ciascuno degli ambiti territoriali di cui si compone l'Azienda, anche con affissioni nei corridoi e/o ingressi principali, la notizia dell'adozione del regolamento informatico aziendale a tutti gli interessati;

• di notificare il presente deliberato a:

- Responsabile UO URP di Potenza, al fine di provvedere alla pubblicazione su Intranet Aziendale del presente atto e del regolamento informatico, di cui lo stesso è parte integrante e sostanziale,

- Responsabile Aziendale UO SIA, al fine di procedere, con adeguati mezzi informatici e nel pieno rispetto della normativa vigente, alla verifica di eventuali anomalie nell'utilizzo di Internet e della Posta Elettronica, da parte dei Lavoratori di questa Azienda, che possono mettere a rischio il sistema di sicurezza informatico;

• di stabilire che, con provvedimento analogo a questo, si procederà alla verifica del regolamento informatico aziendale, al fine di apportare tutte quelle modifiche, che, alla luce di eventuali nuove disposizioni normative di settore e/o progresso tecnologico, appariranno indispensabili per la tenuta di un valido sistema di sicurezza aziendale.

Il presente atto non comporta oneri ed è immediatamente eseguibile, a causa della necessità di procedere alla tempestiva adozione di un unico regolamento informatico, valido per tutto il territorio dell'Azienda.

L'ISTRUTTORE
DRSSA MARIA GRAZIA CLAPS

IL DIRIGENTE RESPONSABILE DELL'UNITÀ OPERATIVA
DR MICHELANGELO MORELLI

IL DIRETTORE SANITARIO
DR. GIUSEPPE NICOLÒ CUGNO

IL DIRETTORE GENERALE
DR. PASQUALE FRANCESCO AMENDOLA

IL DIRETTORE AMMINISTRATIVO
DR. MARIO MARRA

Tutti gli atti ai quali è fatto riferimento nella premessa e nel dispositivo della deliberazione sono depositati presso la struttura proponente, che ne curerà la conservazione nei termini di legge.

OGGETTO Adozione del "REGOLAMENTO AZIENDALE PER L'UTILIZZO DELLE RISORSE INFORMATICHE E TELEMATICHE".

28 MAG. 2010

Si attesta che copia conforme della presente deliberazione è stata trasmessa in data

all'Unità Operativa Responsabile UO URP - Potenza -

e alle Unità Operative Responsabile Aziendale UO SIA - Venosa-

L'IMPIEGATO ADDETTO

(LUIGI MARTORANO)

REGOLAMENTO AZIENDALE PER L'UTILIZZO DELLE RISORSE INFORMATICHE E TELEMATICHE

INDICE

Premessa	pag.	2
1) Utilizzo del personal computer	pag.	3
2) Utilizzo della rete	pag.	5
3) Uso della posta elettronica	pag.	6
4) Memorizzazione temporanea delle informazioni	pag.	7
5) Monitoraggio	pag.	8
6) Informativa ai sensi del d.lgs 196/2003	pag.	9
7) Prescrizioni sulla sicurezza dei dati e dei sistemi	pag.	10

PREMESSA

Le risorse informatiche costituiscono, ormai da tempo, uno strumento di lavoro pressoché indispensabile che le amministrazioni pubbliche e private mettono a disposizione dei dipendenti.
La potenzialità di tali risorse, unitamente alla larga diffusione delle stesse, potrebbe incoraggiarne l'uso anche per finalità diverse da quelle lavorative; non sempre questa evenienza è censurabile, anche alla luce delle direttive volte all'incentivazione dell'utilizzo degli strumenti informatici e telematici nella Pubblica Amministrazione, ma non si possono sottacere i rischi cui può venire esposta l'Amministrazione a causa di usi 'non conformi' di queste risorse, quali ad esempio **rischi di natura patrimoniale** (ad es. il ripristino di danno causato da imperizia o negligenza), **rischi di natura penale** (conseguenti ad es. allo scaricamento di materiale coperto da diritti d'autore); **rischi di perdita o di alterazione di dati**, che nel caso di Organismi Sanitari può causare incidenti tecnici nell'erogazione dei servizi: basti pensare – ad esempio – ai danni che può causare un banale virus informatico che alterasse dati di una refertazione clinica oppure del gruppo sanguigno; **rischi di natura civilistica**, cioè risarcimento del danno agli operatori o agli utenti danneggiati.
Ed è proprio per tutelarsi da questi rischi che le amministrazioni hanno il dovere di emanare regole chiare in grado di delimitare il più possibile i confini tra comportamenti consentiti e comportamenti non consentiti, individuando anche le forme di tutela della propria attività e di autotutela nei confronti di comportamenti che arrecano rischi all'azienda.
È un onere dell'Azienda assicurare la funzionalità degli strumenti messi a disposizione, definendone il corretto utilizzo ed adottando tutte le misure necessarie a garantire sicurezza, disponibilità ed integrità dei sistemi informativi, ma spesso – per la natura stessa delle risorse di cui si discute – l'azione di prevenzione non è sufficiente, e si rende necessario un monitoraggio a vasta scala, che – se non adeguatamente articolato - potrebbe comportare il rischio di venir percepito come strumento di controllo a distanza dell'attività dei lavoratori.

Viceversa questo Regolamento - disciplinante il corretto utilizzo degli strumenti informatici e contenente innanzitutto informazioni utili per comprendere le azioni che ciascun dipendente può mettere in atto per contribuire a garantire la sicurezza informatica di tutta l'Azienda - rappresenta l'osservanza del Provvedimento Generale dal Garante per la Protezione dei Dati Personali del 01.03.2007 pubblicato sulla G.U. del 10.03.2007, n. 58 (Linee guida per posta elettronica e internet) e della Direttiva n. 2 del 26 maggio 2009 della Presidenza del Consiglio dei Ministri - Dipartimento Funzione Pubblica- 'Utilizzo di Internet e della casella di posta elettronica istituzionale sul luogo di lavoro'; la lettura comparata delle due norme, ispirate a principi speculari, rende necessaria l'adozione di questo disciplinare in cui siano definite le regole per l'uso di internet, della posta elettronica e della tenuta di file della rete interna nel pieno rispetto della legge 20.05.1970 n. 300 (Statuto dei Lavoratori) e del D.lgs. 30.06.2003, n. 196 (Codice in materia di protezione dei dati personali) e va preventivamente assoggettato alle procedure di rito, a partire dall'indispensabile concertazione con le rappresentanze sindacali.

Il Personale facente capo al SIA ha il compito di diffondere i contenuti del presente documento e di monitorarne il rispetto nonchè, se indispensabile, di procedere alle verifiche tecniche secondo le modalità di seguito riportate; ma è bene ribadire che **l'attività di monitoraggio e di controllo è finalizzata esclusivamente a prevenire i rischi descritti in precedenza, e viceversa non ha finalità alcuna volta a controllare i lavoratori sul posto di lavoro.**

Art. 1 - UTILIZZO DEL PERSONAL COMPUTER

Il Personal Computer affidato al dipendente è uno strumento di lavoro del quale il dipendente stesso è responsabile; l'utilizzo non inerente l'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione, minacce alla sicurezza.
Non è consentita l'attivazione della password d'accensione (bios), senza preventiva autorizzazione da parte del Personale SIA.
Non è consentito al dipendente modificare le caratteristiche hardware e software impostate sul proprio PC, salvo preventiva autorizzazione da parte del Personale SIA.
Tranne il caso di necessità specifiche, il personal computer deve essere spento alla fine del turno di lavoro o comunque in caso di assenza prolungata durante la giornata lavorativa.
Le informazioni archiviate nel PC devono essere esclusivamente quelle previste dalla legge o necessarie all'attività lavorativa.
Costituisce buona regola la verifica periodica (possibilmente semestrale) degli archivi, con eventuale cancellazione dei file obsoleti o inutili.
La tutela della gestione di dati su personal computer che gestiscono **localmente** documenti e/o dati è demandata all'utente finale che dovrà effettuare, con frequenza opportuna, i salvataggi su supporti magnetici e/o di rete e la conservazione degli stessi in luogo idoneo. In caso di dati sensibili l'uso di supporti rimovibili per la memorizzazione dei dati è ammesso esclusivamente per finalità strettamente connesse con l'attività lavorativa specifica.
Le gestioni locali delle banche dati saranno progressivamente sostituite da gestioni centralizzate su server per consentire l'attivazione ed il rispetto delle misure minime di sicurezza in maniera affidabile e persistente.
Non è consentita l'installazione di programmi diversi da quelli autorizzati dal SIA.
Non è consentita la duplicazione di programmi informatici soggetti a copyright (Legge 128/2004).
Gli operatori del SIA possono richiedere all'Utente la rimozione di file o applicazioni ritenuti pericolosi per la sicurezza, anche attingendo ad appositi elenchi che man mano verranno resi noti agli utenti; in caso di inerzia da parte dei dipendenti, la rimozione avverrà da parte degli operatori del SIA in presenza del dipendente stesso.

Le **password** di accesso a rete e programmi in rete nonché ad internet sono attribuite inizialmente dal SIA; il dipendente dovrà modificare la password al primo utilizzo, e successivamente con cadenza periodica di sei o tre mesi (a seconda della tipologia di dati trattati), consegnando in busta chiusa le proprie password ai custodi di password che verranno indicati; in caso di necessità il custode delle password – su richiesta del dirigente di struttura o del Direttore Generale – renderà disponibile l'accesso alla macchina, informando tempestivamente l'incaricato dell'intervento effettuato, affinché questi provveda a modificare la password.
L'utente è tenuto a conservare con la massima segretezza tutte le password che utilizza; egli è inoltre tenuto a scollegarsi dal sistema ogni qualvolta sia costretto ad assentarsi dal locale nel quale è ubicata la stazione di lavoro e non sia in grado di presidiare l'accesso alla medesima: lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.
La password deve essere immediatamente sostituita - dandone comunicazione al SIA - nel caso si ritenga che la stessa abbia perso il carattere della segretezza.
In caso di accesso alla rete aziendale tramite VPN/accesso remoto, utilizzare l'accesso in forma personale utilizzando esclusivamente le proprie credenzialai di accesso, disconnettendosi dalla rete al termine della sessione di lavoro.

Ogni utente è tenuto a controllare la presenza ed il regolare funzionamento del software antivirus aziendale, e nel caso in cui il software antivirus rilevasse 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 SIA.
È necessario collegarsi periodicamente alla rete interna per consentire il caricamento dell'aggiornamento dell'antivirus.

Utilizzo dei computer portatili

L'utente è responsabile del portatile assegnato dall'azienda e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
Ai portatili si applicano le regole di utilizzo previste per i p.c. in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.
In caso di momentaneo allontanamento i portatili utilizzati all'esterno (convegni ecc.) devono essere custoditi in luogo protetto.
Il portatile non va mai lasciato incustodito; sul disco fisso vanno conservati esclusivamente documenti strettamente necessari.

Utilizzo di cellulari con connessione internet

L'utente è responsabile del cellulare assegnato dall'azienda e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo.
Ai cellulari si applicano le regole di utilizzo previste per i portatili, per quanto compatibili.

Art. 2 - UTILIZZO DELLA RETE AZIENDALE

Per motivi di sicurezza (accesso indesiderato da postazioni esterne) non sono consentiti l'accesso e la navigazione internet se non a mezzo della rete aziendale e per fini esclusivamente lavorativi; è vietato l'utilizzo di modem personali se non espressamente e formalmente autorizzati dal SIA.
È vietato istallare apparati wireless per creazione di reti interne alla U.O., seppure protette, se non dietro esplicita e formale autorizzazione del SIA.
È vietato connettere in rete stazioni di lavoro se non dietro esplicita e formale autorizzazione del SIA; è analogamente vietato condividere cartelle in rete, anche se dotate di password, se non dietro esplicita e formale autorizzazione del SIA.
E' vietato monitorare ciò che transita in rete.
E' consentito navigare in internet unicamente in siti attinenti lo svolgimento delle mansioni assegnate.
Non è consentita, per fini privati, l'effettuazione di qualsiasi genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti online e simili, salvo casi espressamente autorizzati dalla Direzione Aziendale per il tramite del SIA.
Non è consentito lo scaricamento di software gratuiti e shareware prelevati da siti internet, salvo casi espressamente autorizzati dal SIA.
E' consentita la registrazione unicamente a siti i cui contenuti siano legati all'attività lavorativa.
La partecipazione a Forum e bacheche elettroniche e le registrazioni in guestbook sono consentite unicamente per motivi professionali.
La partecipazione a forme di social networking in forma di chatline come, ad esempio, Facebook, GMAIL, MSN Messenger etc. è espressamente vietata in ogni sua forma.
Non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, condizioni di salute, opinione e appartenenza sindacale e/o politica.
Non è consentito l'uso e la navigazione su siti tipo Xrated, Casinò virtuali, Webchat basate su Java, siti Warez e similari.
Non è consentito scaricare/scambiare materiale coperto da diritto d'autore (musica, film, software ecc.).
Il dipendente si impegna ad utilizzare per il proprio lavoro soltanto computer di proprietà dell'azienda, salvo espressa autorizzazione del SIA. Tutti gli strumenti informatici saranno utilizzati esclusivamente per scopi lavorativi, ogni diverso utilizzo che non sia connesso all'attività lavorativa svolta e alle mansioni assegnate è vietato.

Art. 3 - UTILIZZO DELLA POSTA ELETTRONICA

L'abilitazione alla posta elettronica deve essere richiesta al SIA. Una volta attivata la casella, occorre ricordare che la personalizzazione dell'indirizzo di posta elettronica non comporta la sua "privatezza", trattandosi comunque di strumenti di esclusiva proprietà aziendale dati in gestione al dipendente al solo scopo di svolgere le proprie mansioni lavorative, e pertanto non è consentito utilizzare l'indirizzo di posta elettronica aziendale per motivi non attinenti allo svolgimento delle mansioni assegnate: in particolare non è consentito l'utilizzo dell'indirizzo di posta elettronica aziendale per inviare o memorizzare messaggi (interni o esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, condizioni di salute, opinione e appartenenza sindacale e/o politica.
Non è consentita la trasmissione a mezzo posta elettronica di dati sensibili, personali e/o commerciali di alcun genere se non nel rispetto delle norme sulla disciplina del trattamento e della protezione dei dati.
In caso di mittenti sconosciuti o messaggi insoliti, per non correre il rischio di essere infettati da virus occorrerà cancellare i messaggi senza aprire né il messaggio né eventuali documenti allegati: ciò anche allo scopo di evitare che la diffusione incontrollata di messaggi a diffusione capillare limiti l'efficienza del sistema di posta.
In caso di messaggi provenienti da mittenti conosciuti ma che contengono allegati sospetti (file con estensione, exe, ser,) questi ultimi non devono essere aperti.
In caso di invio di allegati informaticamente 'pesanti' è opportuno utilizzare formati compressi (cosiddetti 'zip').
Qualora si debba inviare un documento all'esterno dell'azienda è preferibile utilizzare un formato protetto di scrittura (cifratura), ad evitare che il documento – se intercettato da estranei – possa esser conosciuto.
L'iscrizione a mailing list esterne è ammessa solo per motivi professionali, pertanto prima di iscriversi occorre verificare se il sito è affidabile; in caso di dubbi consultare il SIA.
La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.
È necessario controllare gli allegati di posta elettronica prima del loro utilizzo, evitando di scaricare file eseguibili o documenti da siti non conosciuti.
Tutti i messaggi di posta elettronica inviati relativi alle attività lavorative dovranno contenere un avvertimento ai destinatari di seguito specificato: "si segnala che il presente messaggio e le risposte allo stesso potranno essere conosciute dall'organizzazione lavorativa di appartenenza del mittente secondo le modalità previste dal regolamento aziendale adottato in materia. Se per un disguido avete ricevuto questa e-mail senza esserne i destinatari vogliate cortesemente distruggerla e darne informazione all'indirizzo mittente".

Art. 4 - MEMORIZZAZIONE TEMPORANEA DELLE INFORMAZIONI

Al fine di verificare la funzionalità, la sicurezza del sistema ed il suo corretto utilizzo, le apparecchiature di rete preposte al collegamento verso internet memorizzano un giornale (file di log) contenente le informazioni relative ai siti che i PC aziendali hanno visitato. Tale archivio memorizza l'indirizzo fisico delle postazioni di lavoro e non i riferimenti dell'utente, garantendone in tal modo l'anonimato.
L'accesso a questi dati – detenuti presso la Regione Basilicata, mantainer del servizio a seguito dell'adesione dell'ASP alla RUPAR - è riservato al personale SIA ed eventualmente a personale tecnico esterno autorizzato dalla Direzione Aziendale.
I sistemi software sono programmati e configurati in modo da conservare i dati relativi agli accessi ad internet ed al traffico telematico per il tempo ritenuto strettamente necessario al perseguimento delle finalità organizzative, produttive, di sicurezza e di controllo dell''Azienda, stimato in un mese, dopo di che i dati vengono automaticamente cancellati; il fornitore di servizi internet (cosiddetto ISP, 'Internet Service Provider') detiene invece i dati per un tempo di 2 anni, così come regolamentato da normative comunitarie (direttiva 2006/24/CE del Parlamento Europeo) e nazionali (D. Lgs. n. 109/2008 di recepimento della direttiva comunitaria).

Art. 5 - MONITORAGGIO

L'Azienda Sanitaria di Potenza, nella sua qualità di datore di lavoro, si riserva la facoltà di effettuare controlli in conformità alla legge, anche saltuari od occasionali, sia per eseguire verifiche sulla funzionalità e sicurezza del sistema, sia per verificare il corretto utilizzo da parte dei propri dipendenti tanto della rete internet quanto della posta elettronica; tali controlli costituiscono esclusivamente una misura di sicurezza finalizzata ad evitare i rischi cui si accennava in premessa, e non hanno come finalità il controllo a distanza dell'attività dei lavoratori.
I predetti controlli si svolgeranno in forma graduata secondo le seguenti procedure:
- in via preliminare, l'Azienda provvederà ad eseguire controlli sui dati aggregati, riferiti ad un'intera struttura lavorativa ovvero a sue aree: in caso di riscontro positivo si emanerà un avviso generalizzato inerente l'utilizzo anomalo rilevato degli strumenti aziendali presso l'area/struttura monitorata; tale avviso deve contenere la previsione che, in caso di successivo permanere di situazione non conforme, l'ASP, dopo aver informato il Dirigente di struttura, procederà ad un'analisi puntuale delle singole postazioni di lavoro, eventualmente rimuovendo materiale non consentito, come software, modem e così via;
- consumati i passaggi suddetti (compresa la rimozione di hardware o software non consentiti), in caso di ulteriore reiterato uso non conforme delle risorse informatiche, il personale demandato alle verifiche segnalerà il comportamento del dipendente al Dirigente di struttura, il quale potrà attivare il procedimento disciplinare.

Art. 6 - INFORMATIVA AI SENSI DELL'ART.13 D.LGS. 196/2003.

L'Azienda Sanitaria di Potenza, TITOLARE del trattamento dei dati personali derivanti dall'utilizzo di strumenti elettronici da parte dei lavoratori, intende attivare azioni di monitoraggio finalizzate alla tutela del patrimonio mobiliare nonchè del patrimonio informatico ed informativo.

FINALITA' del trattamento è la verifica del corretto utilizzo della risorse informatiche e telematiche nel rapporto di lavoro.

MODALITA' di trattamento: il personale SIA e personale tecnico esterno autorizzato dal Direttore Generale possono effettuare il trattamento dei dati mediante strumenti informatici. Il trattamento deriva dal monitoraggio che viene effettuato con gradualità e per aree aggregate, e pertanto normalmente i dati relativi ad 'irregolarità' vengono trattati in forma aggregata, senza riferimento al singolo lavoratore.

COMUNICAZIONE DEI DATI: qualora si accerti un reiterato uso indebito delle risorse informatiche ne verrà data comunicazione al Responsabile della U.O. di competenza per la valutazione del caso sotto il profilo disciplinare.

RISPETTO DELLO STATUTO DEI LAVORATORI.
In ossequio al 2^ comma dell'art. 4 della Legge 300/1970 (cd. Statuto dei Lavoratori) il presente documento è stato preventivamente oggetto di concertazione con le Rappresentanze Sindacali Aziendali.

DIRITTI DELL'INTERESSATO: il dipendente potrà far valere i diritti di cui all'art. 7 del D.lgs 196/03 facendo pervenire richiesta scritta alla U.O. Gestione del Personale.

Art. 7 - PRESCRIZIONI SULLA SICUREZZA DEI DATI E DEI SISTEMI

Per quanto riguarda le misure di sicurezza si rimanda al DPS (Documento Programmatico sulla Sicurezza) adottato dall'ASP con atto n._____ del _____ e aggiornato con cadenza annuale.