Letto, confermato e sottoscritto

Il Segretario
Filannino Filomena

Il Direttore Generale
Tommaso Moretti

Il presente provvedimento è stato trasmesso al Collegio dei Revisori il _____

IL SEGRETARIO

CERTIFICATO DI PUBBLICAZIONE

N. 1249

Si certifica che il presente provvedimento è stato pubblicato all'Albo Pretorio dell'Azienda Ospedaliera "Ospedali Riuniti" di Foggia dal 24-5-2010 e per giorni quindici.

Foggia, li 24-5-2010

IL SEGRETARIO

Regione Puglia

OSPEDALI RIUNITI
Azienda Ospedaliero - Universitaria

FOGGIA

Deliberazione del Direttore Generale

Nominato con Delibera di Giunta Regionale n. ~~1251~~ del ~~6/9/05~~ 2224 13/11/2008

N. 210 del Registro

OGGETTO: Aggiornamento del Documento Programmatico sulla sicurezza dei dati personali e del regolamento informatico per l'anno 2010.

L'anno 2010 il giorno 24... del mese di...MAGGIO....., nella sede della Azienda Ospedaliera "Ospedali Riuniti", il Direttore Generale Dott. Tommaso Moretti, con la partecipazione del Direttore Amministrativo e dal Direttore Sanitario, con l'assistenza del Segretario redigente Sig.ra Filannino Filomena, sulla base dell'istruttoria espletata dall'ufficio competente, che attesta la legittimità e conformità della proposta alla vigente normativa, adotta il provvedimento che segue:

Premesso che:

- L'Azienda, con atto deliberativo n. 259 del 31 maggio 2007 ha approvato il Regolamento Informatico con cui si ritenuto necessario
  - stabilire dei principi a cui i dipendenti devono attenersi nell'utilizzo della strumentazione informatica;
  - stabilire i criteri e livelli di accesso ai servizio di navigazione nella rete Internet;
  - stabilire dei criteri di concessione della posta elettronica aziendale

- L'azienda, con atto deliberativo n. 117 del 17 marzo 2010 ha approvato l'aggiornamento del documento programmatico sulla sicurezza dei dati;

Considerato che

- L'Azienda, ha provveduto all'adeguamento della rete dati migliorando le prestazioni di comunicazione portandola a Gb;
- L'azienda, ha attivato servizi di sicurezza perimetrale quali Content filtering, Antispam, Firewall e un monitoraggio esterno da parte del SOC di Telecom s.p.a;
- Internet rappresenta sempre più lo *"Strumento Informatico"* con cui gli operatori devono svolgere le proprie mansioni (ricerche di mercato, approfondimenti tecnici, condivisioni di pareri /consulenze, accesso ad applicativi interaziendali, accessi a Ministeri etc..);

Acquisiti:

- i pareri favorevoli dei Direttori Sanitario ed Amministrativo;

D E L I B E R A

Grafiche DIGIMAIL - Foggia

1. di approvare il nuovo Regolamento Informatico in cui è previsto l'accesso ad Internet a tutti gli Amministrativi, Tecnici e Sanitari dell'Azienda a cui vengono rilasciati le credenziali di accesso al Sistema Informativo Aziendale a seguito di richiesta dei Dirigenti delle Strutture Amministrative / Sanitarie / Tecniche senza limiti orari e/o giornalieri;

2. di notificare il presente atto, in uno con il documento allegato, Dirigenti delle Strutture Amministrative / Sanitarie / Tecniche.

Il presente provvedimento, non essendo soggetto al controllo previsto dalla vigente normativa, è esecutivo ai sensi di legge.

L'Amministratore di Sistema — Dott. Giuseppe Piccolo

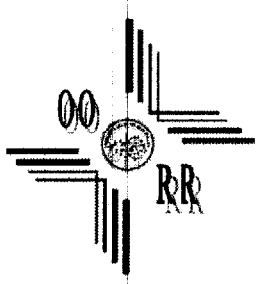
IL DIRETTORE AMMINISTRATIVO — Dott. Giuseppe Cordisco

IL DIRETTORE SANITARIO — Dott. Deni Aldo Procaccini

La presente deliberazione contiene n. ..... (
allegat... ..... che cons... ... di n. .....

Azienda Ospedaliero-Universitaria OSPEDALI RIUNITI FOGGIA Segreteria

IL SEGRETARIO
FILANNINO FILOMENA



Regione Puglia

O S P E D A L I R I U N I T I

Azienda Ospedaliero – Universitaria

F O G G I A

"Regolamento Informatico"

Azienda Ospedaliero-Universitaria "OO.RR." Foggia

STAMPATO IL 20/04/2010

Indice

01. **Premessa**

La progressiva diffusione delle nuove tecnologie informatiche ed, in particolare, l'accesso alla rete Internet dai Personal Computer con comportamenti inconsapevoli possono creare problemi alla sicurezza e all'immagine dell'Azienda stessa.

Premesso che l'utilizzo delle tecnologie informatiche dell'Azienda deve sempre ispirarsi al principio della *diligenza e correttezza* l'Azienda adotta il presente *regolamento* per contribuire alla massima diffusione della cultura della sicurezza. Inoltre, esso si aggiunge e integra le norme già previste dal "Documento Programmatico della Sicurezza" adottato e annualmente aggiornato dall'Azienda.

02. **Utilizzo di Personal Computer, portatili, periferiche e programmi**

Il Personal Computer affidato al dipendente è uno strumento di lavoro. Ogni utilizzo non correlato con l'attività lavorativa, oltre a configurarsi come attività non lecita, può contribuire ad innescare disservizi, costi di manutenzione e minacce alla sicurezza dell'intera rete.

Il SIA nell'ambito della propria attività di gestione del sistema provvede, utilizzando le tecniche e gli strumenti opportuni, a dotare:

- tutti i personal computer di un sistema operativo windoxs xp professional, di antivirus, di sistemi applicativi (video scrittura, fogli elettronici etc..), di applicativi SIA, di connessione alla rete ospedaliera e registrazione nel dominio aziendale;

Non è consentito agli assegnatari dei personal computer, senza la preventiva approvazione tecnica del SIA di :

- installare o far installare altri programmi oltre a quelli in dotazione;
- rimuovere quelli esistenti o modificare la configurazione del sistema;
- installare altre periferiche (H.D., schede audio e video, antenne wi-fi, access point ecc.) oltre a quelle in dotazione;
- installare e/o utilizzare modem per il collegamento con altre reti siano esse pubbliche o private;
- installare e/o utilizzare Hub, Switch e Router per connettere in rete più personal computer (una presa dati un accesso);
- la riproduzione o la duplicazione di programmi informatici ai sensi della legge n.128 del 21.05.2004.

Si precisa, inoltre, che la sicurezza dei dati e/o file locali è demandata ad ogni singolo utente che dovrà effettuare, con frequenza opportuna, i salvataggi su supporti magnetici (CD e /o DVD).

I tecnici del SIA possono in qualunque momento procedere alla rimozione di ogni file, software, hardware che violano le regole del presente regolamento e minacciano la sicurezza dei dati aziendali e/o compromettono le funzionalità di tutti gli apparati informatici connessi alla rete.

03. Gestione della password

Ogni dipendente per poter utilizzare il personal computer connesso alla rete ospedaliera (V-Lan Ospedaliera) deve:

1. sul sito aziendale nella sezione Richiesta Intervento SIA richiedere le credenziali di autenticazioni al sistema informativo indicando nel motivo di intervento "Autorizzazione all'accesso". La richiesta deve essere necessariamente formalizzata, sul sito aziendale, da un Dirigente medico e/o un suo delegato.

2. Il SIA provvede a rilasciare le credenziali d'accesso al Sistema Informativo, nel seguente modo
   - **Identificativo Nome Utente** (Nome): prima lettera del nome di battesimo seguito dal cognome (le eccezioni saranno gestite dal SIA)
   - **Password**: la password di sistema assegnata al primo accesso sarà composta dal giorno/mese per esteso (prima lettera maiuscola)/anno del giorno in cui viene formulata la richiesta Es. (18/Marzo/2010)
3. Da quel momento l'utente che ha fatto richiesta è responsabile della propria password ed è tenuto a:
   - modificare la password al primo accesso, questo processo garantisce la segretezza della stessa;
   - conservare con diligenza e riservatezza le credenziali di accesso alla rete ospedaliera;
   - disconnettersi dal sistema ogni qualvolta sia costretto ad allontanarsi dal personal computer. Lasciare un personal computer 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.
   - modificare la propria password ogni due mesi o nel caso in cui si sospetti che la stessa abbia perso la segretezza. Si precisa che il limite di due mesi è impostato da sistema pertanto se non viene cambiata alla scadenza, occorrerà richiedere le autorizzazioni d'accesso.

04. Utilizzo della Posta Elettronica

- L'abilitazione alla posta elettronica deve essere preceduta da regolare richiesta di un dirigente e/o suo delegato sul sito aziendale nella sezione "Richiesta Intervento Sia";
- l'e-mail, assegnata dall'Azienda, è uno strumento di lavoro e come tale non deve essere usato a fini diversi rispetto alla normale attività lavorativa;

Si precisa che è attivo un servizio antispam (spam significa posta-spazzatura, a rimarcare la sgradevolezza prodotta da tale molestia digitale).

Tipologia di posta elettronica

Personale: individua in modo univoco la persona proprietaria della cassetta e può essere

assegnate esclusivamente a:

- Direttore Generale
- Direttore Sanitario
- Direttore Amministrativo
- Direttori di Struttura complessa
- Dirigenti Medici
- Coordinatori Caposala
- Rappresentanti Sindacali
- Personale amministrativo
- Personale Tecnico

06. Utilizzo di Internet

- L'abilitazione ad Internet verrà rilasciata ad ogni utente che farà richiesta delle credenziali d'accesso preceduta da regolare richiesta di un dirigente medico e/o suo delegato sul sito aziendale;
- la connessione ad Internet è fornita agli utenti abilitati esclusivamente come uno strumento aziendale necessario allo svolgimento della propria attività lavorativa;
- è fatto divieto all'utente lo scarico (download) di software coperto da diritto d'autore;
- è tassativamente vietato l'utilizzo di Internet per effettuare ogni genere di transazione finanziaria (operazioni di remote banking, acquisti on-line e simili);
- è da evitare: ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa, come la partecipazione a forum non professionali, l'utilizzo di chat-line e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames);
- è tassativamente proibito utilizzare i calcolatori e l'infrastruttura di rete Aziendale allo scopo di connettersi ad Internet nei circuiti P2P. Tali circuiti sono prevalentemente utilizzati dagli utenti per lo scambio abusivo di materiali protetti dal diritto di autore ovvero per scaricare e/o condividere filmati, canzoni e programmi;
- sono espressamente vietate le connessioni ad Internet su linea telefonica, con modem ed abbonamenti personali;
- ai Dirigenti, ai Responsabili di Servizio e ai Dirigenti medici e/o suo delegato è demandato l'obbligo di vigilare al fine di garantire che la connessione ad Internet venga utilizzata nel rispetto di quanto sopra.

Si precisa, inoltre, che sono state attività misure di sicurezza perimetrale (Content filtering, Antispam, Firewall e un monitoraggio esterno per individuare eventuali attacchi informatici e valutare le vulnerabilità interne) necessarie a garantire il buon funzionamento della rete dati dell'Azienda.

La navigazione in Internet non è anonima: la semplice visualizzazione di una pagina web comporta la registrazione dell'evento in una base dati di sistema (proxy server aziendale) in cui sono memorizzati i siti visitati, la data e ora di connessione, l'utente connesso ed il tempo di connessione.

06. Verifica dell'utilizzo della posta elettronica e di Internet

Si informano i dipendenti titolari di password che questa Amministrazione, in ottemperanza ai principi di necessità, correttezza, pertinenza e non eccedenza, potrà procedere a verifica dell'utilizzo

dell'accesso ad Internet e della posta elettronica in maniera anonima e preliminare su dati aggregati.

".. Il controllo anonimo può concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite. L'avviso può essere circoscritto a dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia. In assenza di successive anomalie non è di regola giustificato effettuare controlli su base individuale" (Garante Privacy Del. n.13 del 1° Marzo 2007).

07. **Osservanza delle norme**

Si ricorda a tutti gli utenti del Sistema Informativo dell'Azienda Ospedaliero – Universitaria di Foggia, siano essi dipendenti o collaboratori, che è obbligatorio attenersi alle disposizioni in materia di privacy e di misure minime di sicurezza ai sensi del D.L. 196/2003 e del Documento Programmazione dell'Azienda Ospedaliero – Universitaria di Foggia.

08. **Non Osservanza delle norme**

Il mancato rispetto del D.L. 196/2003 e del DPS o la violazione delle regole contenute nel presente regolamento costituiscono inosservanza delle disposizioni, nel qual caso il personale può essere oggetto di provvedimenti disciplinari ai sensi della vigente normativa contrattuale, nonché nei casi più gravi di azioni civili e/o penali - ove consentite - nei confronti dei trasgressori.

Allegato composto di n. Tre

alla deliberazione n. 340 del 24-5-2010

Azienda Ospedaliero-Universitaria • Segreteria • OSPEDALI RIUNITI FOGGIA

IL SEGRETARIO
FILANNINO [illegible]