



*REGOLAMENTO INTERNO PER UN CORRETTO USO DELLE INFRASTRUTTURE E  
DELLE RISORSE INFORMATICHE DELL'AZIENDA OSPEDALIERA OSPEDALI  
RIUNITI VILLA SOFIA - CERVELLO*

UOC Servizio Tecnico – Servizio Informatico Aziendale

**Data**  
06.08.2012

**Pagina**  
1

*REGOLAMENTO INTERNO PER UN CORRETTO USO DELLE  
INFRASTRUTTURE E DELLE RISORSE INFORMATICHE DELL'AZIENDA  
OSPEDALIERA OSPEDALI RIUNITI VILLA SOFIA - CERVELLO*

**LISTA DI DISTRIBUZIONE**


Direttore Generale

Direttore Sanitario


Direttore Amministrativo

Direttori UU.OO

<b>Rev.</b>	<b>Data</b>	<b>Causale</b>	<b>Redazione</b>	<b>Verifica</b>	<b>Approvazione DG</b>
01	06.08.2012	Prima stesura	Servizio Informatico Aziendale	UOC Servizio Tecnico	Delibera n.1529 del 09.08.2012

 <p><b>AZIENDA OSPEDALIERA</b> OSPEDALI RIUNITI VILLA SOFIA - CERVELLO PALERMO</p>	<p><i>REGOLAMENTO INTERNO PER UN CORRETTO USO DELLE INFRASTRUTTURE E DELLE RISORSE INFORMATICHE DELL'AZIENDA OSPEDALIERA OSPEDALI RIUNITI VILLA SOFIA - CERVELLO</i></p>	
<p>UOC Servizio Tecnico – Servizio Informatico Aziendale</p>	<p><b>Data</b> 06.08.2012</p>	<p><b>Pagina</b> 2</p>

1. Scopo .....	3
2. Campo di applicazione .....	5
3. Terminologia .....	5
4. Responsabilità.....	5
5. Utilizzo delle risorse informatiche .....	7
a. Utilizzo della rete informatica aziendale (RIA).....	7
b. Utilizzo del Personal Computer .....	7
c. Gestione delle credenziali di accesso .....	8
d. Utilizzo dei supporti esterni di memorizzazione.....	9
e. Salvataggio e ripristino dei dati .....	9
f. Utilizzo della posta elettronica.....	9
g. Uso della rete internet e dei relativi servizi.....	10
h. Protezione antivirus .....	12
6. Integrazioni, correzioni e validità .....	12

 <p><b>AZIENDA OSPEDALIERA</b> OSPEDALI RIUNITI VILLA SOFIA - CERVELLO PALERMO</p>	<p><i>REGOLAMENTO INTERNO PER UN CORRETTO USO DELLE INFRASTRUTTURE E DELLE RISORSE INFORMATICHE DELL'AZIENDA OSPEDALIERA OSPEDALI RIUNITI VILLA SOFIA - CERVELLO</i></p>	
<p>UOC Servizio Tecnico – Servizio Informatico Aziendale</p>	<p><b>Data</b> 06.08.2012</p>	<p><b>Pagina</b> 3</p>

## 1. Scopo

Il presente documento fornisce le linee guida principali e le regole per un corretto uso delle infrastrutture e delle risorse informatiche **dell'Azienda Ospedaliera Ospedali Riuniti Villa Sofia - Cervello** di Palermo che, per brevità, nel prosieguo del presente documento verrà denominata **"Azienda"**.

I dispositivi hardware e software acquisiti dall'Azienda nonché la rete di trasmissione dati e tutti gli accessori ad essa collegati, consentendo l'accesso, l'elaborazione e la distribuzione delle informazioni sia all'interno che all'esterno di essa, costituiscono strumenti indispensabili per la corretta gestione delle attività istituzionali connessi alla mission Aziendale.

L'Azienda assegna in uso al personale dipendente, inserito nel proprio organigramma dispositivi ed attrezzature informatiche e ne promuove l'utilizzo ritenendole strategiche per le attività amministrative e di gestione dell'organizzazione Sanitaria Aziendale.


Gli utenti della rete e delle risorse informatiche messe a disposizione dall'Azienda sono tenuti a farne un corretto uso, ad averne cura e a rispettare ed osservare, nello specifico, le regole stabilite nel presente regolamento.

L'Azienda adotta un Sistema di Gestione della Sicurezza ICT in linea con le necessità e gli obiettivi strategici, i requisiti di sicurezza e la struttura organizzativa al fine di:

- garantire che il patrimonio informativo e informatico sia adeguatamente tutelato rispetto ai rischi di compromissione.
- istituire e mantenere un processo strutturato per l'identificazione e la valutazione del rischio informatico, con lo scopo di applicare gli opportuni controlli e di verificare l'efficacia e l'efficienza in ottica di un miglioramento continuo;
- assicurare la conformità ai requisiti legali e normativi inerenti la sicurezza delle informazioni.

Tali requisiti di sicurezza sono individuati e definiti come segue:

- **Riservatezza:** le informazioni devono essere accessibili solo da parte di chi ha la necessità di conoscerle ed è di conseguenza autorizzato all'accesso; le informazioni devono essere protette ai fini della confidenzialità in ogni fase del ciclo di vita del trattamento.
- **Integrità :** il trattamento delle informazioni deve avvenire assicurando l'accuratezza, la completezza e la protezione degli asset informativi, e che i metodi di elaborazione e trasmissione in rete prevengono ed evitano manomissioni e modifiche da parte di personale non autorizzato.
- **Disponibilità:** gli utenti autorizzati all'accesso agli asset informativi devono poter usufruire del trattamento delle informazioni di competenza nel momento in cui ne hanno necessità.

 <p> <b>AZIENDA OSPEDALIERA</b>  <b>OSPEDALI RIUNITI VILLA SOFIA - CERVELLO</b> PALERMO </p>	<b>REGOLAMENTO INTERNO PER UN CORRETTO USO DELLE INFRASTRUTTURE E  DELLE RISORSE INFORMATICHE DELL'AZIENDA OSPEDALIERA OSPEDALI  RIUNITI VILLA SOFIA - CERVELLO</b>	
UOC Servizio Tecnico – Servizio Informatico Aziendale	<b>Data</b> 06.08.2012	<b>Pagina</b> 4

- **Non ripudiabilità:** garantisce l'identità delle parti coinvolte in uno scambio telematico di informazioni; garantisce altresì l'identità di una persona che firma digitalmente un documento in relazione al contenuto del documento stesso.


Premesso quindi che l'utilizzo delle risorse informatiche e telematiche aziendali deve sempre ispirarsi al principio della diligenza e correttezza, l'Azienda adotterà il presente Regolamento interno al fine di evitare che comportamenti più o meno consapevoli possano innescare particolari problematiche o minacce alla sicurezza nel trattamento dei dati.

La sicurezza delle informazioni riguarda tutta l'azienda coinvolgendo, allo stesso livello di importanza, gli aspetti legati ai sistemi informativi, al personale ed ai processi operativi attraverso una serie di controlli che verifichino e garantiscano il livello di sicurezza raggiunto attraverso i più vari strumenti: policy, procedure, strutture organizzative, strumenti software.

Una corretta politica di gestione delle informazioni trova il suo presupposto nell'esigenza dell'azienda stessa che, resasi conto dell'importanza delle proprie informazioni e definiti i propri specifici obiettivi di sicurezza, cerchi poi di raggiungerli. Tali obiettivi di sicurezza possono – anzi devono – essere quantificati e definiti dall'organizzazione stessa in base alle proprie strategie ad alle caratteristiche del proprio business, ma devono necessariamente essere rapportati e valutati in base a parametri universalmente riconosciuti.

Nel rispetto dei principi di pertinenza e di non eccedenza, i controlli preventivi e continui sull'uso degli strumenti informatici devono garantire tanto il diritto del datore di lavoro di proteggere la propria organizzazione, essendo i computer aziendali strumenti di lavoro per i quali l'utilizzazione personale è preclusa, quanto il diritto del lavoratore a non vedere invasa la propria sfera personale, e quindi il diritto alla riservatezza ed alla dignità così come sancito dallo Statuto dei lavoratori, dalle vigenti disposizioni contrattuali e dal D.lgs 196/03 sulla tutela dei dati personali.

Il Regolamento Aziendale di seguito riportato viene incontro a tali esigenze disciplinando le condizioni per il corretto utilizzo degli strumenti informatici da parte dei dipendenti, in particolare alla luce degli obblighi previsti dal D.lgs 196/2003 relativi all'adozione delle misure minime di sicurezza per il trattamento dei dati personali.

 <p><b>AZIENDA OSPEDALIERA</b> OSPEDALI RIUNITI VILLA SOFIA - CERVELLO PALERMO</p>	<b>REGOLAMENTO INTERNO PER UN CORRETTO USO DELLE INFRASTRUTTURE E DELLE RISORSE INFORMATICHE DELL'AZIENDA OSPEDALIERA OSPEDALI RIUNITI VILLA SOFIA - CERVELLO</b>	
UOC Servizio Tecnico – Servizio Informatico Aziendale	<b>Data</b> 06.08.2012	<b>Pagina</b> 5

## 2. Campo di applicazione

Le regole contenute nel presente documento si applicano a tutto il personale che opera all'interno dell'Azienda mediante l'ausilio di supporti informatici ed in generale a tutti coloro a cui, a qualsiasi titolo, sia concesso l'uso delle risorse informatiche aziendali, sia controllate individualmente che condivise, gestite su un singolo computer o rese disponibili in rete.

Il presente regolamento disciplina, inoltre, le modalità di accesso e di uso della Rete Informatica e telematica dell'Azienda che è costituita dall'insieme delle risorse informatiche aziendali (asset), dalle risorse infrastrutturali e dal patrimonio informativo digitale. Le risorse infrastrutturali sono le componenti hardware/software e gli apparati elettronici collegati alla **Rete Informatica Aziendale (RIA)**. Il Patrimonio informativo è l'insieme delle banche dati in formato digitale ed in generale tutti i documenti prodotti tramite l'utilizzo dei suddetti apparati.

## 3. Terminologia


<b>Sistema informativo</b>	Insieme ordinato di elementi diversi (procedure, risorse umane, mezzi) che raccolgono, elaborano, scambiano e archiviano dati al fine di produrre e distribuire informazioni nel momento e luogo adatto ai soggetti che ne hanno bisogno.
<b>Sistema informatico</b>	Parte del sistema informativo, costituita dall'insieme degli strumenti informatici e organizzativi, necessari per il trattamento automatico delle informazioni di un'organizzazione.
<b>Patrimonio informativo</b>	Insieme dei dati aziendali che hanno subito un qualche processo di raffinamento e da grezzi, sono stati filtrati, sintetizzati, aggregati ed elaborati trasformandosi così in informazioni.

## 4. Responsabilità

Poiché in caso di violazioni contrattuali e giuridiche, sia l'Azienda, sia il singolo lavoratore sono potenzialmente perseguibili con sanzioni, anche di natura penale, l'Azienda verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole e l'integrità del proprio sistema informatico.

Alla luce dell'art.4, comma 1, Legge n. 300/1970 la regolamentazione della materia indicata nel presente regolamento, non è finalizzata all'esercizio di un controllo a distanza dei lavoratori da parte del datore di lavoro, ma solo per permettere all'Azienda di utilizzare i sistemi informativi per far fronte ad esigenze produttive od organizzative e di sicurezza nel trattamento dei dati personali e sanitari.

In conformità a quanto disposto dalla deliberazione n. 13 del 1 marzo 2007 del Garante per la protezione dei dati personali (Gazzetta Ufficiale n. 58 del 10 marzo 2007) si ritiene necessario informare che:


 <p> <b>AZIENDA OSPEDALIERA</b>  <b>OSPEDALI RIUNITI VILLA SOFIA - CERVELLO</b> PALERMO </p>	<b>REGOLAMENTO INTERNO PER UN CORRETTO USO DELLE INFRASTRUTTURE E DELLE RISORSE INFORMATICHE DELL'AZIENDA OSPEDALIERA OSPEDALI RIUNITI VILLA SOFIA - CERVELLO</b>	
UOC Servizio Tecnico – Servizio Informatico Aziendale	<b>Data</b> 06.08.2012	<b>Pagina</b> 6

- Il Servizio Informatico Aziendale, effettua un monitoraggio periodico dell'*hardware presente* e del *software* installato nei PC Aziendali. Il monitoraggio, necessario per finalità organizzative (inventario del parco macchine e contabilità delle licenze d'uso del *software*), non coinvolge in alcun modo i dati personali ed i documenti presenti sui PC, ma permette la rilevazione di *software* installato in violazione di questo regolamento.
- Al fine di prevenire, per quanto ed ove possibile, comportamenti scorretti durante la navigazione in Internet, l'Azienda si avvale di appositi filtri che impediscono l'accesso a siti non ritenuti idonei ed il *download* di *files* multimediali non attinenti all'attività lavorativa. Ciò in osservanza della Direttiva n. 02/09 del 26/05/2009 del Ministro per la Pubblica Amministrazione e l'innovazione.
- L'Azienda, ai soli fini di sicurezza, si riserva di attivare in qualsiasi momento e senza ulteriori comunicazioni agli utenti, un servizio di memorizzazione dei log del proxy server al solo fine di avere la possibilità di risalire all'utente che ha effettuato eventuali attività non autorizzate o illecite all'interno della rete aziendale e su internet, in caso di indagini svolte dalla magistratura. Il controllo e monitoraggio suddetto è disposto anche in applicazione del provvedimento del Garante della Privacy del 27 novembre 2008 recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema.
- I *files di log* contenenti le registrazioni suddette sono conservati per il tempo strettamente necessario, determinato dalle norme in vigore e da esigenze di sicurezza.

Il mancato rispetto o la violazione delle regole contenute nel presente Regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali previste.

Nel caso di inadempimento grave e doloso che metta a repentaglio la sicurezza del sistema informativo Aziendale o vengano poste in essere attività illegali, verranno inoltrate agli organi competenti (Polizia delle Comunicazioni, Autorità giudiziaria) le risultanze di apposita attività di accertamento e verifica di eventuali responsabilità personali a carico di dipendenti resisi colpevoli di reati informatici.

All'atto dell'assegnazione di dispositivi informatici il dipendente dovrà sottoscrivere apposita dichiarazione di presa in carico e in custodia del relativo dispositivo. Dovrà inoltre fornire il proprio consenso informato relativamente all'erogazione dei servizi di assistenza tecnica erogati dall'U.O. a tal fine preposte. Con il predetto atto il dipendente si impegna a custodire il dispositivo Aziendale nel rispetto dei doveri di custodia scaturenti dalle vigenti disposizioni normative in materia di utilizzo di attrezzature appartenenti alla Pubblica Amministrazione impegnandosi inoltre a custodire con cura e diligenza i beni consegnati e a non sostituire, alterare o modificare la configurazione originaria delle medesime attrezzature senza le prescritte autorizzazioni.

 <p><b>AZIENDA OSPEDALIERA</b> OSPEDALI RIUNITI VILLA SOFIA - CERVELLO PALERMO</p>	<p><i>REGOLAMENTO INTERNO PER UN CORRETTO USO DELLE INFRASTRUTTURE E DELLE RISORSE INFORMATICHE DELL'AZIENDA OSPEDALIERA OSPEDALI RIUNITI VILLA SOFIA - CERVELLO</i></p>	
<p>UOC Servizio Tecnico – Servizio Informatico Aziendale</p>	<p><b>Data</b> 06.08.2012</p>	<p><b>Pagina</b> 7</p>

## **5. Utilizzo delle risorse informatiche**

### **a. Utilizzo della rete informatica aziendale (RIA)**

Gli utenti che hanno accesso alla RIA, nel rispetto delle leggi e normative vigenti, devono porre particolare attenzione alle seguenti regole di comportamento:

- utilizzare le risorse con modalità orientate alle finalità dell'organizzazione Aziendale;
- evitare accessi non autorizzati alle risorse;
- evitare di abusare delle risorse comuni, monopolizzandone l'uso o limitandone la disponibilità agli altri utenti;
- rispettare i diritti d'autore ed il copyright, le licenze d'uso e l'integrità di risorse informative basate su Personal computer e dispositivo hardware di diverso tipo;
- rispettare in generale i diritti degli altri utenti che accedono alle risorse del sistema informatico aziendale;
- rispettare i regolamenti di Enti e Strutture che interagiscono con l'Azienda quali Enti previdenziali, Enti territoriali, Assessorato Regionale alla Sanità etc.

La concessione in uso delle risorse informatiche dell'Azienda implica, pertanto, specifiche responsabilità delle strutture coinvolte e dei singoli utenti ed è revocabile in qualsiasi momento per la tenuta di comportamenti e/o attività non conformi a leggi e/o regolamenti nonché alle regole di cui al presente documento.

È inoltre proibito l'uso di computer, reti, attrezzature o servizi di comunicazione elettronica (quali posta elettronica, instant messaging o similari) per inviare, visualizzare o scaricare messaggi che comportino dolo, frode, molestie di qualsiasi natura o altri messaggi o materiale che costituiscano violazioni delle leggi vigenti o da norme regolamentari.


### **b. Utilizzo del Personal Computer**

Il Personal Computer affidato al dipendente costituisce uno strumento di lavoro e come tale ogni utilizzo non inerente l'attività lavorativa cui lo stesso è destinato può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza informatica aziendale.

A tal fine, al momento dell'assegnazione in custodia del medesimo, sarà fatta sottoscrivere al dipendente apposito modulo di presa in carico con contestuale dichiarazione da parte dello stesso di presa visione del presente regolamento e di accettazione di tutte le clausole ivi contenute.

L'accesso all'elaboratore dovrà essere protetto da password che sarà custodita dall'utente con la massima diligenza e non divulgata.

Non è consentito installare autonomamente programmi provenienti dall'esterno salvo autorizzazione esplicita fornita da parte del personale del Servizio informatico Aziendale, in quanto potenzialmente portatrice di virus informatici ed altre tipologie di malware che possono alterare la stabilità delle applicazioni dell'elaboratore e dell'intera rete Aziendale.

 <p> <b>AZIENDA OSPEDALIERA</b>  <b>OSPEDALI RIUNITI VILLA SOFIA - CERVELLO</b>          PALERMO       </p>	<b>REGOLAMENTO INTERNO PER UN CORRETTO USO DELLE INFRASTRUTTURE E          DELLE RISORSE INFORMATICHE DELL'AZIENDA OSPEDALIERA OSPEDALI          RIUNITI VILLA SOFIA - CERVELLO</b>	
UOC Servizio Tecnico – Servizio Informatico Aziendale	<b>Data</b> 06.08.2012	<b>Pagina</b> 8

Non è consentito, inoltre, l'uso di programmi diversi da quelli distribuiti ufficialmente dall'Azienda (D.lgs. 518/92 sulla tutela giuridica del software e L. 248/2000 nuove norme di tutela del diritto d'autore e del copyright). Qualsiasi violazione delle regole di cui alle predette norme comporterà la responsabilità individuale dell'interessato.

Dovranno, inoltre, essere messi in atto accorgimenti tali per cui il computer non resti, durante una sessione di trattamento di gestione dati:

- incustodito: può essere sufficiente che un soggetto non autorizzato rimanga nei locali durante l'assenza di chi sta operando con lo strumento elettronico;
- accessibile: può essere sufficiente attivare lo screen saver con password oppure chiudere a chiave il locale ove è situato lo strumento elettronico, durante l'assenza, anche se nel medesimo locale non rimane nessuno.

Non è consentita l'installazione sul proprio PC di qualunque dispositivo di memorizzazione, comunicazione o altro (come ad esempio, modem, switch, router, access point, ecc. ), se non con l'autorizzazione espressa del personale facente parte del Servizio Informatico.

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.

### **c. Gestione delle credenziali di accesso**

Le credenziali di accesso alla rete, e ai sistemi aziendali devono essere richieste dall'utente attraverso il modulo in allegato firmato dal responsabile dell'UO a cui egli afferisce e sono assegnate dal Servizio Informatico Aziendale o da personale da questo delegato. L'user ID (identificativo dell'utente) deve essere definito in maniera chiara e facilmente collegabile all'utilizzatore.

Al primo accesso l'utente deve provvedere a modificare la password ricevuta. Nel caso di trattamento di dati sensibili sarà obbligato automaticamente alla sostituzione ogni tre mesi.

La password deve essere composta da almeno 8 caratteri alfa numerici (numeri o lettere) di cui almeno 1 numero, 1 lettera maiuscola, 1 lettera minuscola ed 1 carattere speciale quali ad esempio (&-&-&-?^-ç-§-(-)-£). Nella creazione della password dovranno essere rispettati i caratteri maiuscolo e minuscolo.


La password deve essere segreta e quindi non dovrà essere portata a conoscenza a soggetti terzi. Ogni utente dovrà adottare le necessarie cautele per assicurare la sua segretezza. Ad esempio, la password non potrà essere trascritta su post-it da applicare sui monitor dei PC, né riportata sulle prime pagine della propria agenda.

La password, di regola, non deve contenere riferimenti agevolmente riconducibili all'interessato (non solo nomi, cognomi, soprannomi, ma neppure date di nascita proprie, dei figli o degli amici).

La password, utilizzata dagli incaricati al trattamento dei dati, ha una durata massima di mesi sei, trascorsi i quali deve essere sostituita.

Nel caso di trattamento di dati sensibili la password dovrà avere una durata massima di mesi tre, trascorsi i quali deve essere sostituita.



 <p><b>AZIENDA OSPEDALIERA</b> OSPEDALI RIUNITI VILLA SOFIA - CERVELLO PALERMO</p>	<b>REGOLAMENTO INTERNO PER UN CORRETTO USO DELLE INFRASTRUTTURE E DELLE RISORSE INFORMATICHE DELL'AZIENDA OSPEDALIERA OSPEDALI RIUNITI VILLA SOFIA - CERVELLO</b>	
UOC Servizio Tecnico – Servizio Informatico Aziendale	<b>Data</b> 06.08.2012	<b>Pagina</b> 9

**d. Utilizzo dei supporti esterni di memorizzazione**

Tutti i supporti elettronici riutilizzabili (dischetti, cassette, CD, pen drive, cartucce) contenenti dati sensibili devono essere trattati con particolare cautela. Infatti devono essere custoditi (in archivi chiusi a chiave) ed utilizzati in modo tale da impedire accessi non autorizzati (furti inclusi) e trattamenti non consentiti.

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

Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente l'Amministratore di Sistema nel caso in cui siano rilevati virus ed adottando quanto previsto dal presente Regolamento nella sezione relativa alle procedure di protezione antivirus.

**e. Salvataggio e ripristino dei dati**

I dati personali devono essere salvati con cadenza settimanale. Ogni utente è tenuto a controllare PERSONALMENTE il regolare funzionamento dei backup e verificare il salvataggio di tutti i files di pertinenza dell'Azienda presenti nel proprio PC.

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

Per la tutela dei dati gestiti all'interno del Sistema Informativo Aziendale, è attivo un sistema per la gestione dei backup, secondo quanto previsto dalle normative vigenti.


**f. Utilizzo della posta elettronica**

La casella di posta, assegnata dall'Azienda all'utente, è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse. L'abilitazione al servizio di posta elettronica aziendale è messo a disposizione degli utenti dopo la compilazione del modulo, in allegato, firmato dallo stesso e dal responsabile dell'UO a cui egli afferisce.

E' fatto divieto di utilizzare indirizzi email private per comunicazioni inerenti l'attività aziendale.

E' fatto divieto di utilizzare le caselle di posta elettronica Aziendale per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mailing-list non attinenti alle attività lavorative salvo diversa ed formale autorizzazione.

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

 <p><b>AZIENDA OSPEDALIERA</b> OSPEDALI RIUNITI VILLA SOFIA - CERVELLO PALERMO</p>	<p><i>REGOLAMENTO INTERNO PER UN CORRETTO USO DELLE INFRASTRUTTURE E DELLE RISORSE INFORMATICHE DELL'AZIENDA OSPEDALIERA OSPEDALI RIUNITI VILLA SOFIA - CERVELLO</i></p>	
<p>UOC Servizio Tecnico – Servizio Informatico Aziendale</p>	<p><b>Data</b> 06.08.2012</p>	<p><b>Pagina</b> 10</p>

Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per l'Azienda, ovvero contenga documenti da considerarsi riservati in quanto contraddistinti dalla dicitura "strettamente riservati" o da analogha dicitura, deve essere visionata od autorizzata dal proprio dirigente responsabile. In ogni modo, è opportuno fare riferimento alle procedure in essere per la corrispondenza ordinaria. E' possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario.

Per la trasmissione di file all'interno dell'Azienda è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati. E' obbligatorio controllare i file allegati (attachements) di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).


E' vietato inviare catene telematiche. Se si dovessero ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al Servizio Informatico Aziendale. Non si deve in alcun caso attivare gli allegati di tali messaggi.

**g. Uso della rete internet e dei relativi servizi**

Il PC abilitato alla navigazione in Internet costituisce per l'utente assegnatario uno strumento necessario allo svolgimento della propria attività lavorativa. E' assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati ai compiti istituzionali allo stesso attribuiti. A tal fine si rinvia alla Direttiva n. 02/09 del 26/05/2009 emanata dal Ministro della Pubblica Amministrazione e dell'Innovazione che detta le linee guida all'utilizzo di Internet e della posta elettronica istituzionale all'interno dei luoghi di lavoro nell'ambito della pubblica Amministrazione e al provvedimento del Garante per la protezione dei dati personali del 01.03.2007 recante: "Lavoro: le linee guida del Garante per la posta elettronica e Internet".

Per tale ragione l'Azienda è dotata di appositi strumenti informatici che limitino il traffico degli utenti autorizzati alla navigazione (web-filtering) e consenta loro di accedere a siti esclusivamente connessi con l'attività lavorativa svolta. L'accesso ad Internet dovrà essere richiesto dal responsabile della Unità organizzativa cui il dipendente è assegnato su apposita modulistica in Appendice A. Il dipendente dovrà dichiarare di essere a conoscenza del presente regolamento e di accettare incondizionatamente le clausole contenute nell'apposita dichiarazione. Il Dirigente responsabile dell'Unità organizzativa richiedente dovrà inoltre specificare i siti di interesse istituzionale cui il dipendente potrà accedere al fine di espletare compiutamente i propri compiti istituzionali connessi alla propria attività lavorativa.

E' fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dall'Amministratore di Sistema. A tal fine, nell'ambito del miglioramento dei sistemi di sicurezza informatica e tenuto conto delle disposizioni impartite dal Ministero per la Pubblica Amministrazione e l'innovazione, dall'Authority per l'informatica e dagli altri organismi preposti, l'Azienda dispone di appositi strumenti di controllo di tipo hardware e software che saranno opportunamente configurati al fine di impedire accessi non autorizzati alla

 <p><b>AZIENDA OSPEDALIERA</b> OSPEDALI RIUNITI VILLA SOFIA - CERVELLO PALERMO</p>	<p><i>REGOLAMENTO INTERNO PER UN CORRETTO USO DELLE INFRASTRUTTURE E DELLE RISORSE INFORMATICHE DELL'AZIENDA OSPEDALIERA OSPEDALI RIUNITI VILLA SOFIA - CERVELLO</i></p>	
<p>UOC Servizio Tecnico – Servizio Informatico Aziendale</p>	<p><b>Data</b> 06.08.2012</p>	<p><b>Pagina</b> 11</p>

rete aziendale (firewall), attacchi di tipo virale e/o di altri malware (worm, spyware, trojan horse, dialer, backdoor etc.).

Al fine di non pregiudicare il corretto funzionamento del sistema informativo aziendale e nel rispetto delle predette policy di sicurezza, si fa presente che è fatto assoluto divieto per gli utenti di agire deliberatamente con attività che influenzino negativamente la regolare operatività della rete e ne restringano l'utilizzabilità e le prestazioni per altri utenti.

Per tale motivo è espressamente vietato far uso di programmi di file-sharing e/o peer to peer, effettuare download massivi di prodotti multimediali, prodotti musicali che violino anche i diritti di autore, procedere all'installazione ed utilizzo di software di qualsiasi tipo e a qualsiasi fine scaricato dal web anche se trattasi di software di tipo freeware o open source.

L'installazione di software sui computer dell'Azienda prelevato dalla rete sia residente su altri supporti, è permessa unicamente se destinata ad estendere le funzionalità native del browser (plug-in, activeX ecc.) e può avvenire solo ed esclusivamente con l'autorizzazione del Servizio informatico Aziendale.

Inoltre si fa presente che la navigazione sulla rete Internet non può essere utilizzata per scopi vietati dalla legislazione vigente.

Si ribadisce che, nei casi in cui fossero accertati comportamenti contrari alle regole di cui al presente regolamento da parte degli utenti abilitati secondo le modalità sopra indicate e da ciò ne derivassero danni patrimoniali a carico dell'Azienda, si procederà, con le modalità di cui alle vigenti disposizioni normative.


Se fossero inoltre provati e verificati anche comportamenti perseguibili in sede penale si precisa che di ciò ne saranno informati gli organi Giudiziari competenti e gli organi di Polizia Postale per l'accertamento di quanto accertato.

E' tassativamente vietata 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 dall'Azienda e con il rispetto delle normali procedure di acquisto. E' da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.

E' vietata, inoltre, 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). È fatto altresì divieto di utilizzo di Social forum o sistemi di chat personale (Facebook, Twitter, Windows Messenger o similari).

Il Servizio Informatico Aziendale si riserva di applicare per singoli e gruppi di utenti politiche di navigazione personalizzate in base alle mansioni ed eventuali disposizioni concordate con la Direzione e con i Dirigenti, al fine di ottimizzare l'uso delle risorse, gli investimenti e le prestazioni delle connessioni esistenti.

Non è consentita 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.

 <p><b>AZIENDA OSPEDALIERA</b> OSPEDALI RIUNITI VILLA SOFIA - CERVELLO PALERMO</p>	<p><i>REGOLAMENTO INTERNO PER UN CORRETTO USO DELLE INFRASTRUTTURE E DELLE RISORSE INFORMATICHE DELL'AZIENDA OSPEDALIERA OSPEDALI RIUNITI VILLA SOFIA - CERVELLO</i></p>	
<p>UOC Servizio Tecnico – Servizio Informatico Aziendale</p>	<p><b>Data</b> 06.08.2012</p>	<p><b>Pagina</b> 12</p>

E' fatto assoluto divieto di utilizzo di connessioni attraverso Internet Key, chiavette USB o dispositivi di connessione PMCIA o similari per la navigazione su rete internet su PC o Notebook connessi alla rete aziendale, se non autorizzate dal Servizio Informatico Aziendale.

#### **h. Protezione antivirus**

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.

Nel caso che il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente:

- a) sospendere ogni elaborazione in corso senza spegnere il computer;
- b) segnalare l'accaduto al Servizio informatico Aziendale

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 consegnato all'amministratore di sistema.

Nell'ambito dei miglioramenti della sicurezza in ambito ICT, l'Azienda provvede a predisporre un sistema di aggiornamento automatico degli antivirus installati in ciascuna postazione.

#### **6. Integrazioni, correzioni e validità**

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

Copia del regolamento verrà altresì pubblicato sul sito internet Aziendale all'indirizzo: [www.ospedaliriunitipalermo.it](http://www.ospedaliriunitipalermo.it) Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi ogni dipendente e collaboratore in possesso di specifiche credenziali di autenticazione; tale figura potrà anche essere indicata come "incaricato" o "incaricato del trattamento".

Si fa riserva di adottare successive eventuali integrazioni o correzioni alle disposizioni del presente regolamento, in relazione all'entrata in vigore di sopravvenute normative ed all'evolversi della tecnologia.

Il presente Regolamento è soggetto a revisione con frequenza annuale o qualora si verificassero particolari necessità che rendano inapplicabili o non più conformi una o più parti di esso.