"Linee Guida per l'utilizzo della rete, dei servizi informatici e della Posta Elettronica"

In considerazione di quanto prescritto dal Garante della Privacy ai datori di lavoro Pubblici e Privati nell'ambito delle Linee Guida per Posta Elettronica ed Internet, pubblicate in data 01 Marzo 2007 – Bollettino 81, appare opportuno specificare le modalità di utilizzo, da parte dei lavoratori, degli strumenti messi a loro disposizione, nonché le modalità con cui vengono effettuati i controlli. Tali Linee Guida vengono quindi proposte preventivamente alle OO.SS. nel rispetto dei principi che regolano le relazioni sindacali stesse trattandosi di fatti che impattano sull'organizzazione del lavoro e sui diritti dei lavoratori stessi. Le linee giuda assumono il ruolo di disciplinare interno, opportunamente pubblicizzato, attraverso la stessa rete, ed soprattutto in funzione del Documento Programmatico sulla Sicurezza
Posto che ogni Unità Operativa è connessa in rete, i lavoratori, preventivamente autorizzati, sono dotati di dispositivi per l'accesso alla rete aziendale ed eventuale accesso ad Internet utilizzando le postazioni indicate ed assegnante dai rispettivi Responsabili. Con lo stesso disciplinare sono state adottate misure di tipo tecnologico e procedurale tese ad una sicura "navigazione in Internet" ed un corretto utilizzo della posta elettronica nel rispetto di un corretto trattamento dei dati personali nei casi in cui gli stessi debbano essere utilizzati (se non sensibili) per il perseguimento di un legittimo interesse del datore di lavoro.

Articolo 1
OGGETTO E AMBITO DI APPLICAZIONE

Il presente regolamento disciplina le modalità di accesso e di uso delle attrezzature, delle apparecchiature, della rete informatica dell' Azienda Ospedaliera "Pugliese Ciaccio" di Catanzaro, a sua volta connessa alla rete Internet, nonché dei servizi che, tramite la stessa rete, è possibile ricevere e offrire, il tutto compatibilmente con il progressivo sviluppo dei servizi e con la progressiva implementazione di tutti i sistemi di sicurezza, tenuto conto delle risorse messe a disposizione dall'Azienda e della continua evoluzione della tecnologia informatica.

Articolo 2
PRINCIPI GENERALI – DIRITTI E RESPONSABILITÀ

1. L' Azienda Ospedaliera "Pugliese Ciaccio" di Catanzaro promuove l'utilizzo della rete dei servizi informatici e telematici (*la rete*, nel seguito) quale strumento utile per perseguire le proprie finalità e individua nel Settore Sistemi Informativi, afferente all'Area di Staff Programmazione – Controllo, il servizio stesso a cui affidarne, la gestione, la manutenzione e l'evoluzione.

2. I soggetti autorizzati come da Art. 5 ad accedere alla rete (*gli utenti* della rete, nel seguito) utilizzano le risorse e i servizi della rete nel rispetto dell'integrità dei sistemi, in osservanza delle leggi, norme e obblighi contrattuali.

3. Ogni utente è responsabile del diligente mantenimento delle attrezzature informatiche utilizzate, al fine di preservarne funzionalità ed efficienza. In particolare deve anche provvedere allo spegnimento delle attrezzature in uso, al termine del suo orario di lavoro, se non sono necessarie ad altri utenti. Il diligente mantenimento delle attrezzature comporta anche l'obbligo di aprire e scaricare quotidianamente la posta elettronica al fine di evitare il blocco della casella stessa.

4. Ogni utente e' tenuto ad operare ponendo attenzione al contenimento del consumo di materiali informatici quali supporti per la memorizzazione dei dati (floppy disc, CD, DVD, etc.) e cartucce e toner di stampanti, privilegiando l'uso e la diffusione del documento elettronico rispetto a quello cartaceo.

5. Gli utenti, consapevoli delle potenzialità offerte dagli strumenti informatici e telematici, si impegnano ad agire con responsabilità e a non commettere abusi aderendo ad un principio di autodisciplina. Con il termine di abuso si intende qualsiasi violazione del presente regolamento e di altre norme civili, penali e amministrative che disciplinano le attività e i servizi svolti sulla rete e di condotta personale che saranno diffusi anche successivamente quali aggiornamento delle presenti linee guida.

6. Ogni postazione di lavoro informatizzata viene assegnata completa dei dispositivi (*hardware*) e dei programmi di base e degli applicativi specifici (*software*), necessari per svolgere le funzioni di base richieste dall'attività dell'ufficio, d'intesa con il Dirigente/Responsabile del Servizio interessato, e compatibilmente con le licenze d'uso disponibili e le risorse economiche e strumentali dell'Azienda. E' pertanto vietato agli utenti modificarne la configurazione di base e installare, modificare, rimuovere o spostare qualsiasi attrezzatura o dispositivo hardware e installare, rimuovere o alterare qualsiasi software di qualunque tipo e origine. A tal fine sarà necessario, custodire scrupolosamente i CD di installazione consegnati con la macchina. Ciò al fine di consentire e garantire le operazioni di eventuale reinstallazione e/o soddisfare i controlli delle autorità preposte.

7. Tutte le richieste di installazioni, realizzazioni e ristrutturazioni hardware e software devono essere valutate congiuntamente dal Dirigente/Responsabile del Servizio interessato e dal Responsabile del Settore Sistemi Informativi, o dal suo incaricato, cui spetta la verifica tecnica della compatibilità degli strumenti richiesti con l'infrastruttura di rete e la normativa vigente, con particolare riferimento alla sicurezza delle banche dati dell'Azienda. In particolare, non possono essere effettuate realizzazioni, ristrutturazioni, acquisizioni e installazioni di attrezzature e/o componenti hardware e/o software senza preventiva valutazione, visto tecnico o istruttoria della pratica nei limiti di delega del Settore Sistemi Informativi. Nel caso in cui gli strumenti proposti non possano, per ragioni tecniche, essere installati, saranno individuate, ove possibile e nei limiti della tecnologia, soluzioni alternative,

tecnicamente fattibili, d'intesa tra il Settore Sistemi Informativi e il servizio/U.O. interessato. Gli strumenti e i sistemi hardware/software tecnicamente utilizzabili saranno resi disponibili dal Settore Sistemi Informativi (o da personale tecnico da questa esplicitamente autorizzato), compatibilmente con le licenze d'uso disponibili e le risorse economiche e strumentali dell'Azienda. I software acquistati a partire dalla data di emanazione del presente regolamento e le relative licenze sono di norma conservati e registrati su apposito registro presso il Settore Sistemi Informativi (ex C.E.D.), così da consentire le operazioni di verifica della disponibilità di licenze e l'eventuale installazione o conservate presso il Responsabile dell' U.O., che firma per ricevuta con l'obbligo della custodia delle stesse.

8. Ogni utente è responsabile della conservazione dei dati e dei documenti elettronici di qualsiasi tipo, formato e natura che utilizza, sia sulla propria postazione di lavoro informatizzata che su altre, se, per esigenze d'ufficio, è in regime di condivisione di risorse. Per questo motivo ogni utente è tenuto ad effettuare la copia periodica di questi dati e documenti. In caso di guasto, malfunzionamento o sostituzione di una postazione di lavoro informatizzata, nonchè di cancellazioni o modifiche accidentali, potranno essere recuperati soltanto i documenti preventivamente salvati. Qualsiasi documento non preventivamente salvato a cura dell'utente, non potrà in alcun caso essere recuperato, con possibile danno per l'Ente.

Articolo 3
ABUSI E ATTIVITÀ VIETATE

E' vietato ogni tipo di abuso, secondo quanto definito all' Art. 2 del presente regolamento. In particolare è vietato:

1. usare la rete in modo difforme da quanto previsto dalle leggi penali, civili e amministrative e da quanto previsto dal presente regolamento;
2. utilizzare la rete per scopi personali o incompatibili o non inerenti con l'attività istituzionale dell' Azienda Ospedaliera "Pugliese Ciaccio" di Catanzaro;
3. utilizzare una credenziale di autenticazione personale (nome utente e/o password o smart-card) a cui non si è autorizzati;
4. cedere a terzi credenziali di autenticazione personali (nome utente e/o password o smart-card) di accesso ai sistemi informatici;
5. conseguire l'accesso non autorizzato a risorse di rete interne o esterne alla rete dell' Azienda Ospedaliera "Pugliese Ciaccio" di Catanzaro;
6. violare la riservatezza di altri utenti o di terzi;
7. agire deliberatamente con attività che influenzino negativamente la regolare operatività della rete e ne restringano l'utilizzabilità e le prestazioni per altri utenti (es.: uso di programmi di file-sharing e/o p2p, etc.);
8. effettuare o permettere ad altri trasferimenti non autorizzati di informazioni (software, licenze, dati, etc.);
9. utilizzare software o servizi di cui non si disponga della licenza d'uso;

10. installare o eseguire deliberatamente o diffondere su qualunque computer e sulla rete, programmi destinati a danneggiare, sovraccaricare i sistemi o la rete o carpire informazioni e dati (es.: virus, dialer, etc.)
11. cancellare, disinstallare, copiare, spostare o asportare programmi e componenti hardware/software o licenze d'uso;
12. installare componenti e/o programmi software senza l'autorizzazione del Settore Sistemi Informativi (es.: stampanti, tastiere, lettori MP3, software di terze parti, etc.)
13. utilizzare caselle di posta elettronica e servizi "Web-Mail" non direttamente riconducibili all' Azienda Ospedaliera "Pugliese Ciaccio" di Catanzaro @aocz.it (es.: caselle e/o servizi quali yahoo, hotmail, tiscali, etc.)
14. utilizzare la posta elettronica e i servizi Internet inviando e/o ricevendo materiale che violi le leggi o non attinente alle finalità ed alla mission aziendale;
15. Saturare la casella di posta elettronica, per negligenza nelle procedure di scarico quotidiano della stessa, tanto da rendere impossibile la ricezione di comunicazioni istituzionali;
16. collegarsi a siti e/o servizi Internet non inerenti l'attività dell'ufficio e/o dell'Azienda;
17. adottare comportamenti non tollerati quali il download di software o di file musicali e/o video;
18. aprire o salvare in qualsiasi formato e su qualsiasi supporto messaggi di posta elettronica, il cui oggetto sia marcato con la dicitura "VIRUS" o altra dicitura simile.
19. accedere direttamente ad Internet e/o a reti e servizi esterni con modem collegato alla propria postazione informatizzata, se non espressamente autorizzati dal Settore Sistemi Informativi e per particolari motivi tecnici;
20. utilizzare sistemi o servizi personali di messaggistica (instant messaging), di chat, di telefonia su Internet (VOIP) o simili se non autorizzati;
21. monitorare o utilizzare qualunque tipo di servizio e sistema informatico o elettronico per controllare le attività degli utenti, leggere, copiare o cancellare file e software di altri utenti, senza averne l'autorizzazione;
22. usare l'anonimato o servirsi di risorse che consentano di restare anonimi sulla rete;
23. modificare password di accesso ai sistemi e ai servizi;
24. abbandonare la postazione informatizzata, lasciandola incustodita e accessibile, ovvero, se accessibile, senza aver verificato l'attivazione del servizio di salvaschermo protetto da password.

Articolo 4
ATTIVITÀ CONSENTITE

1. Agli utenti sono consentite tutte le attività non espressamente vietate dalla legge, dal presente regolamento o da altri provvedimenti dell'Azienda.

2. Il Settore Sistemi Informativi, per il corretto svolgimento dei suoi compiti istituzionali e per finalità di ricerca e sviluppo necessarie alla crescita

dell'infrastruttura di rete e dei servizi informatici dell'Ente, può derogare dai divieti del presente regolamento, fermo restando il rispetto degli obblighi normativi.
In particolare, al Settore Sistemi Informativi è anche consentito:

a) Monitorare o utilizzare qualunque tipo di servizio e sistema informatico o elettronico per controllare il corretto utilizzo delle risorse di rete (postazioni informatizzate e componenti software), per copiare o rimuovere file e software, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori. In particolare è consentito al Settore Sistemi Informativi, al fine di garantire un efficiente livello di servizio, l'utilizzo di servizi e sistemi di "Teleassistenza", che consentono al personale del Settore Sistemi Informativi, o a personale tecnico di terze parti, da questa esplicitamente autorizzato, di accedere da remoto alle postazioni informatizzate. In questo caso l'operatore alla postazione informatizzata sottoposta a Teleassistenza sarà avvisato, o telefonicamente o tramite altre forme ritenute idonee, al momento dell'intervento stesso;
b) Monitorare o utilizzare qualunque tipo di servizio e sistema informatico o elettronico per supervisionare indirettamente la navigazione Internet e il traffico di posta elettronica, sia per esigenze statistiche che di controllo della spesa e dell'utilizzo dei servizi. L'attività di monitoraggio consiste esclusivamente nel tenere traccia, per ogni postazione di lavoro informatizzata, del nome della pagina Internet visitata, e degli indirizzi di destinazione e provenienza dei messaggi di posta elettronica. Il contenuto delle pagine Internet visitate e dei messaggi di posta elettronica entranti/uscenti non sono in alcun modo soggetti a monitoraggio, in accordo al principio di autodisciplina espresso dall'Art. 2 e dalle Linee Guida del Garante della Privacy emesse quale provvedimento a carattere generale in data 01 Marzo 2007 (Bollettino n° 81 Marzo 2007);
c) Privilegiare meccanismi di controllo preventivo su dati aggregati fermo restando la possibilità di effettuare verifiche di comportamenti anomali attraverso misure specifiche;
d) Adottare le necessarie misure tecniche preventive (firewall e Server Proxy) e/o a posteriori, per garantire un adeguato livello di sicurezza della rete, incluso il blocco temporaneo o definitivo della navigazione su siti Internet e/o su domini di posta elettronica. In accordo al principio di autodisciplina espresso dall'Art. 2, e nel rispetto delle attività vietate all'Art.3, la fruizione di Internet e della Posta Elettronica risulta libera, e ogni utente è responsabile della navigazione e dello scambio di messaggi dalla postazione di lavoro assegnatagli. Ciascun utente potrà utilizzare i servizi di Posta Elettronica per ragioni personali in misura limitata all'essenziale. Al Settore Sistemi Informativi è demandato, compatibilmente con quanto la tecnologia consente, di effettuare controlli indiretti, saltuari o occasionali, per i quali saranno avvisati tutti i fruitori preventivamente via e-mail indicando motivazioni e modalità dei controlli stessi, nonchè di attivare i meccanismi idonei ad interdire i siti Internet il cui accesso comporta palesemente la violazione degli Artt. 2 e 3. In caso di rischi riconosciuti per la sicurezza del sistema informativo dell'Ente (diffusione di virus, etc), il Servizio Informativo, su sua iniziativa e previa autorizzazione del Responsabile d'Area potrà chiudere qualsiasi sito, ma soltanto

temporaneamente, per la sola durata dell'emergenza, e comunicando tempestivamente a tutti gli uffici la durata presunta del blocco.

Articolo 5

SOGGETTI CHE POSSONO AVERE ACCESSO ALLA RETE E AI SERVIZI

1. Hanno diritto ad accedere alla rete del Azienda Ospedaliera "Pugliese Ciaccio" di Catanzaro:
   a) i dipendenti, se autorizzati dal Dirigente/Responsabile del Servizio cui sono assegnati ai quali viene assegnato un indirizzo e-mail e/o IP;
   b) i collaboratori esterni impegnati nelle attività istituzionali per il periodo di collaborazione, se autorizzati dal Dirigente/Responsabile del Servizio interessato;
   c) il Direttore Generale ed i Direttori Sanitario ed Amministrativo, per la durata del mandato istituzionale;
   d) il personale tecnico di terze parti per motivi di manutenzione ordinaria/straordinaria e limitatamente alle applicazioni, ai servizi e all'infrastruttura di competenza per il periodo necessario all'intervento, se espressamente autorizzato dal Settore Sistemi Informativi;

2. L'accesso alla rete è assicurato compatibilmente con le potenzialità delle attrezzature e nei limiti imposti dalla tecnologia, tramite il rilascio, ai soggetti autorizzati, di credenziali di autenticazione (coppie utente/password o simili) da parte del Servizio Informativo - Area Programmazione e Controllo.

3. Con l'obiettivo di garantire un adeguato livello di sicurezza e il miglior funzionamento delle risorse di rete disponibili, il Settore Sistemi Informativi può:
   a) regolamentare l'accesso alla rete di determinate categorie di utenti, quando questo è richiesto da ragioni tecniche;
   b) adottare apposite disposizioni di carattere operativo che gli utenti si impegnano ad osservare.

4. L'accesso ai servizi e ai programmi applicativi è consentito solo agli utenti che hanno accesso alla rete e che, per motivi di servizio, ne devono fare uso.

5. Le password di accesso ai sistemi informativi (software applicativi e banche dati) vengono rilasciate e revocate esclusivamente dal Servizio Informativo (delegato per le password) solo e soltanto su richiesta dei Dirigenti/Responsabili dei Servizi, cui quei sistemi e/o quelle banche dati fanno riferimento.

6. Ad ogni variazione del personale assegnato ad un ufficio, i Dirigenti/Responsabili dei Servizi coinvolti, ciascuno per la propria competenza, devono comunicare al Settore Sistemi Informativi il nominativo del personale da variare e i servizi informativi per i quali assegnare o revocare la credenziale di accesso (password).

7. Ad ogni variazione delle mansioni del personale assegnato ad un ufficio, il Dirigente/Responsabile del Servizio deve comunicare al Settore Sistemi Informativi

il nominativo del personale da variare e i servizi informativi per i quali assegnare o revocare la credenziale di accesso (password).

8. I soggetti che accedono alla rete e ai servizi informatici devono richiedere al Settore Sistemi Informativi la sostituzione delle proprie credenziali di accesso nel caso in cui sia stata compromessa la loro riservatezza e almeno una volta ogni sei mesi, salvo diverse disposizioni interne o di legge.

9. In particolare possono essere individuati uno o più responsabili del trattamento dei dati e della manutenzione del sistema i quali dovranno porre opportuna cura nel prevenire l'accesso a dati personali presenti in cartelle o in spazi di memoria, svolgendo solo operazioni strettamente necessarie e senza realizzare attività di controllo a distanza non autorizzate preventivamente. Per tale motivo manutentori interni, responsabili del trattamento e amministratore di sistema o figure analoghe dovranno svolgere specifica attività formativa sui profili gestionali, tecnici e di sicurezza delle reti e sui principi di protezione dei dati personali e del segreto nella comunicazione.

Articolo 6
MODALITÀ DI ACCESSO ALLA RETE E AI SERVIZI

1. Qualsiasi accesso alla rete e ai servizi informatici viene associato ad una persona fisica o ad un'entità giuridica, cui sono attribuite le attività svolte utilizzando le credenziali di autenticazione assegnategli. Tutte le attività svolte sono registrate elettronicamente e soggette a supervisione per esigenze statistiche, di controllo della spesa e a garanzia del livello di sicurezza della rete.

2. L'utente che ottiene l'accesso alla rete e ai servizi si impegna ad osservare il presente regolamento e le altre norme disciplinanti le attività e i servizi che si svolgono via rete e si impegna a non commettere abusi e a non violare i diritti degli altri utenti e dei terzi, assumendosi la totale responsabilità delle attività svolte.

3. Ad ogni utente autorizzato come da Art. 5 del presente regolamento sono assegnate e comunicate dal Settore Sistemi Informativi:
   a) una password di accensione della postazione informatizzata normalmente utilizzata come da indicazione del Dirigente/Responsabile del Servizio interessato; tale password, su richiesta, può essere comunicata al Responsabile dell'Ufficio per consentire l'accesso alla postazione da parte del personale dell'ufficio stesso.
   b) le credenziali (nome utente e password) per l'accesso alla rete informatica da qualsiasi postazione informatizzata. Tali credenziali sono strettamente personali, in quanto identificano in maniera univoca chi accede alla rete e ai servizi dell'Azienda, incluse le banche dati. Ciascun utente deve adottare le necessarie cautele per assicurarne la segretezza e la diligente custodia. Il Responsabile del Servizio/U.O. può custodire o richiedere una copia di queste credenziali, da usare nel caso di assenza o impedimento che renda indispensabile e indifferibile

intervenire, accedendo con quelle credenziali, per esclusiva necessità operativa. In tal caso, immediatamente superata la necessità, deve essere richiesto all'ufficio Sistemi Informativi la sostituzione delle credenziali divulgate.

c) L'Utente deve individuare, in caso di assenza improvvisa e/o prolungata, un suo sostituto (fiduciario) in grado di accedere alla sua casella di posta elettronica capace di verificare il contenuto e l'avvio, al titolare del trattamento dei dati, di quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Sarà cura del Titolare del trattamento la redazione di apposito verbale al fine di informare il lavoratore alla prima occasione utile.

Articolo 7
SANZIONI

In caso di abuso, a seconda della gravità del medesimo, e fatte salve ulteriori conseguenze di natura penale, civile e amministrativa, possono essere comminate le sanzioni disciplinari previste dalla normativa vigente in materia e dai regolamenti dell' Azienda Ospedaliera "Pugliese Ciaccio" di Catanzaro distinguendo tra personale del comparto e della Dirigenza ai sensi di quanto previsto dai rispettivi CC.CC.NN.LL. che qui si intendono totalmente richiamati.

Il Responsabile Settore Sistemi Informativi
(Dott. Pier Raffaele Martorelli)

Il Dirigente Responsabile
Area Programmazione e Controllo
(Dott. Sergio Petrillo)