Regione del Veneto

AZIENDA SANITARIA – U.L.S.S. N. 3

(istituita con L.R. n. 56 del 14.9.1994)

sede: Bassano del Grappa – via Carducci n. 2

cod. s.i.s. 050 – 103

N. **1640** /Reg. del D.G. Bassano del Grappa, **28/12/2004**

DELIBERAZIONE
del

DIRETTORE GENERALE

Nominato con D.P.G.R. n. 1511 del 31.12.2002.

Coadiuvato dai sigg.:

DIRETTORE AMMINISTRATIVO dott. GERVASIO MILANI

DIRETTORE SANITARIO dr. FRANCESCO PIETROBON

DIRETTORE DEI SERVIZI SOCIALI dott. ALESSANDRO PIGATTO

OGGETTO: Servizio Affari Generali – D.L.vo n. 196/2003: approvazione documento contenente regole di comportamento per una corretta gestione della privacy e della sicurezza nei luoghi di lavoro.

Premesso che con D.Lgs. n. 196/03 è stato approvato il nuovo codice in materia di protezione dei dati personali, con abrogazione secondo il disposto dall'art. 183 del medesimo D.Lgs., di quasi tutte le norme contenute nell'apparato normativo previgente;

Dato atto che nel disciplinare tecnico in materia di misure minime di sicurezza (all. B al D.Lgs. medesimo) sono previsti interventi informativi e formativi per rendere edotti gli Incaricati del trattamento dei dati dei rischi individuati e dei modi per prevenire possibili danni, con riferimento anche alla custodia ed accessibilità ai locali;

Ritenuto, in attesa della definizione di un piano di formazione che sarà ricompreso nel DPS (Documento Programmatico sulla Sicurezza) in via di elaborazione, di individuare un pacchetto di regole comportamentali alle quali gli Incaricati del trattamento sono tenuti ad uniformarsi;

Visto l'allegato documento, predisposto dal Servizio competente, contenente regole di comportamento per una corretta gestione della privacy e della sicurezza nei luoghi di lavoro;

Ricordato che:
- con precedente delibera n. 1495 del 15.12.2004 sono stati individuati i Responsabili del trattamento dati di cui all'art. 29 del D.Lgs. 196/03;
- con delibera n. 1545 del 22.12.2004 è stato approvato il documento di Informativa di cui all'art. 13 del medesimo D.Lgs. n. 196/03;

Ricordato, altresì, che sono in via di attivazione incontri di formazione con i Responsabili del trattamento dati, con supporto della Ditta Polimatica Progetti s.r.l. (rif. delibera n. 1377 del 17.11.2004) finalizzati a consentire il censimento delle risorse (fisiche e logiche), l'analisi dei rischi e l'individuazione delle misure di sicurezza ai fini di pervenire, entro il prossimo mese di febbraio, alla stesura del DPS;

Sentito il Direttore Amministrativo, il quale dà atto che il servizio competente ha attestato l'avvenuta regolare istruttoria della pratica, in ordine alla compatibilità con la vigente legislazione statale, regionale e regolamentare;

Visto l'art. 32 della L.R. 9.9.1999 n. 46, recante nuove disposizioni sul controllo degli atti delle Aziende Sanitarie;

Acquisito il parere favorevole dei Direttori per quanto di rispettiva competenza;

DELIBERA

1. di approvare, per le finalità riportate in premessa, l'allegato documento contenente "**Regole di comportamento"** per una corretta gestione della privacy e della sicurezza nei luoghi di lavoro dell'Azienda Sanitaria ULSS n. 3, in conformità alle disposizioni recate dal D.Lgs. n. 196/03.

2. di disporre che tale documento venga trasmesso, oltre che ai Direttori delle Articolazioni Aziendali, ai Responsabili del trattamento dati come individuati con delibera n. 1495 del 15.12.2004, ai fini della distribuzione del documento stesso agli Incaricati del trattamento e con obbligo, per entrambi, di adeguamento alle regole di comportamento previste.

3. di dare atto che la presente deliberazione viene pubblicata all'albo dell'Azienda per 10 gg. continuativi, inviata contestualmente al Collegio Sindacale e diventa esecutiva il giorno stesso della sua pubblicazione, come da norma regolamentare approvata con provvedimento n. 1711 del 13.12.2000.

Regole di comportamento

per una corretta gestione della privacy
e della sicurezza nei luoghi di lavoro

1. ***Chiudere a chiave cassetti ed uffici***. Il primo livello di protezione di qualunque sistema è quello fisico. E' certamente vero che una porta chiusa può, in molti casi, non costituire una protezione sufficiente, ma è anche vero che pone, se non altro, un primo ostacolo, e richiede comunque uno sforzo volontario non banale per la sua rimozione. È fin troppo facile per un estraneo entrare in un ufficio non chiuso a chiave e sbirciare documenti posti su una scrivania o visibili su uno schermo. Pertanto, chiudete a chiave il vostro ufficio alla fine della giornata ed ogni volta che vi assentate. Inoltre chiudete i documenti a chiave nei cassetti ogni volta che potete.

2. ***Non lasciare documenti sulla scrivania***. Non lasciate documenti, lettere, fascicoli, appunti sopra la scrivania quando vi allontanate dalla postazione di lavoro. In particolare, non lasciate sul tavolo materiali che non siano inerenti alla pratica che state trattando in quel momento. Ciò vale soprattutto nel caso in cui abbiate mansioni di front-office e di ricezione del pubblico.

3. ***Spegnere il computer se ci si assenta per un periodo di tempo lungo***. Lasciare un computer acceso non crea problemi al suo funzionamento e, al contrario, velocizza il successivo accesso. Tuttavia, un computer acceso è, in linea di principio, maggiormente attaccabile perché raggiungibile tramite la rete o direttamente sulla postazione di lavoro. Inoltre, più lungo è il periodo di assenza, maggiore è la probabilità che un'interruzione dell'energia elettrica possa portare un danno.

4. ***Non lasciare lavori incompiuti sullo schermo***. Chiudete sempre le applicazioni con cui state lavorando quando vi allontanate dal posto di lavoro per più di pochi minuti: potreste rimanere lontani più del previsto e un documento presente sullo schermo è vulnerabile (quasi) quanto uno stampato o copiato su dischetto.

5. ***Salvaschermo***. Ogni postazione di lavoro deve avere il salvaschermo attivato, con richiesta di password per poter riprendere il controllo della postazione (da Windows XP, clicca sul desktop col tasto destro del mouse, apri proprietà, vai su screen server e spunta la casella "al ripristino proteggi con password").

6. ***Proteggere attentamente i dati***. Bisogna prestare particolare attenzione ai dati importanti di cui si è personalmente responsabili. Poiché può risultare difficile distinguere tra dati normali e dati importanti, è buona norma trattare tutti i dati come se fossero importanti. Come minimo, posizionarli in un'area protetta da password e non dare la default a nessun altro utente il permesso di lettura o modifica. Ai dati da condividere, applicare i permessi opportuni solo per il tempo strettamente necessario all'interazione con gli altri utenti.

7. ***Conservare supporti di memoria e stampe in luoghi sicuri***. Alla conservazione dei supporti di memoria (CD, dischetti) si applicano gli stessi criteri di protezione dei documenti cartacei, con l'ulteriore pericolo che il loro smarrimento (che può anche essere dovuto a un furto) può passare più facilmente inosservato. A meno che non siate sicuri che contengano solo informazioni non sensibili, riponeteli sotto chiave non appena avete finito di usarli.

8. ***Maneggiare e custodire con cura le stampe di materiale riservato***. Non lasciate accedere alle stampe persone non autorizzate. Se la stampante non si trova sulla vostra scrivania recatevi il più in fretta possibile a ritirare le stampe. Per stampe riservate, cercate di usare una stampante non condivisa oppure usate la modalità di stampa ritardata impostando un tempo sufficiente a permettervi di raggiungere la stampante prima dell'inizio della stampa. Distruggete personalmente le stampe quando non servono più anche se sono solo delle "brutte copie" o bozze da ristampare perché errate.

9. ***Prestare attenzione alle fotocopie***. Fate fotocopie di documenti contenenti dati personali sensibili solo se strettamente necessario. Assicuratevi di non lasciare copie nella macchina e, se necessario, eliminate copie mal riuscite utilizzando una macchina distruggi-documenti (shredder), qualora esista.

10. ***Non gettare nel cestino le stampe di documenti che possono contenere informazioni confidenziali***. Se trattate dati di particolare riservatezza, considerate la possibilità di dotarvi di una macchina distruggi-documenti (shredder). In ogni caso non gettate mai documenti cartacei senza averli prima fatti a pezzi.

11. ***Non riutllizzare i dischetti per affidare a terzi i vostri dati***. Quando un file viene cancellato da un disco magnetico, i dati non vengono effettivamente eliminati dal disco ma soltanto marcati come non utilizzati e sono facilmente recuperabili. Neanche la formattazione assicura l'eliminazione dei dati dai

dischi. Solo l'uso di un apposito programma di cancellazione sicura garantisce che sul dischetto non resti traccia dei dati precedenti. Nel dubbio, è sempre meglio usare un dischetto nuovo.

12. ***Prestare particolare attenzione all'utilizzo dei computer portatili***. I PC portatili sono un facile bersaglio per ladri. Se avete necessità di gestire dati riservati su un portatile, proteggetelo con una password sul BIOS, fate installare un programma di cifratura del disco rigido (per impedire la lettura dei dati in caso di furto) ed effettuate periodicamente il back up.

13. ***Proteggere il proprio computer con una password***. Abilitate, ove possibile, l'accesso tramite password. La maggior parte dei computer offre la possibilità di impostare una password all'accensione. Anche alcuni applicativi permettono di proteggere i propri dati tramite password. Imparate a utilizzare queste caratteristiche che offrono un buon livello di riservatezza.

14. ***Fare attenzione a non essere spiati mentre si digita una password o qualunque codice di accesso***. Anche se molti programmi non ripetono in chiaro la password sullo schermo, quando digitate una password questa potrebbe essere letta guardando i tasti che state battendo, anche se avete buone capacità di dattiloscrittura. Chiedete agli astanti di guardare da un'altra parte quando introducete una password o controllate che nessuno stia guardando.

15. ***Non permettere l'uso del proprio account ad altri colleghi d'ufficio***. Non comunicate la vostra password di accesso al PC a nessuno, né tanto meno a colleghi di ufficio. Un'attività illecita svolta da un vostro collega con la vostra Password sarà attribuita a Voi, con tutte le conseguenze giuridiche del caso.

16. ***Non permettere l'uso del proprio computer o del proprio account a personale esterno***, a meno di non essere sicuri della loro identità. Personale esterno può avere bisogno di installare software/hardware nuovo nel vostro computer. Assicuratevi dell'identità della persona e delle autorizzazioni ad operare sul vostro PC.

17. ***Non utilizzare apparecchiature non autorizzate o per cui non si è autorizzati***. L'utilizzo di modem su postazioni di lavoro collegate alla rete di ufficio offre una porta d'accesso dall'esterno non solo al vostro computer, ma a tutta la rete di cui fate parte. E' quindi vietato l'uso di modem all'interno della rete locale. Nel caso che ciò sia strettamente necessario, disconnettete fisicamente la postazione di lavoro dalla rete locale prima di effettuare il collegamento via modem. Per l'uso di altre apparecchiature, chiedete consiglio all'amministratore di sistema.

18. ***Non installare programmi non autorizzati***. Oltre alla possibilità di trasferire involontariamente un virus o di introdurre un cosiddetto "cavallo di troia", va ricordato che la maggior parte dei programmi sono protetti da copyright, per cui la loro installazione può essere illegale.

19. ***Diffidare dei dati o dei programmi la cui provenienza non è certa***. Per proteggersi da virus ed altri agenti attivi di attacco, diffidate di tutti i dati e programmi che vi vengono inviati o consegnati, anche se la fonte appare affidabile o il contenuto molto interessante. Infatti, molti sistemi di attacco inviano dati che sembrano provenire da un utente noto al destinatario per vincerne la naturale diffidenza nei confronti degli estranei.

20. ***Applicare con cura le linee guida per la prevenzione di infezioni da virus***. La prevenzione delle infezioni da virus sul vostro computer è molto più facile e comporta uno spreco di tempo molto minore rispetto alla correzione degli effetti di un virus. Inoltre, se non avete attivato adeguate misure anti-virus, potreste incorrere in una perdita irreparabile di dati o in un blocco anche molto prolungato della vostra postazione di lavoro.

21. ***Usare, se possibile, il salvataggio automatico dei dati***. Non dimenticare i salvataggi volontari. Molti programmi applicativi, ad esempio quelli di videoscrittura, salvano automaticamente il lavoro a intervalli fissi, in modo da minimizzare il rischio di perdita accidentale dei dati. Imparate comunque a salvare manualmente il vostro lavoro con una certa frequenza, in modo da prendere l'abitudine di gestire voi stessi i dati e non fare esclusivo affidamento sul sistema.

22. ***Non violare le leggi in materia di sicurezza informatica***. Ricordatevi che anche solo un tentativo di ingresso non autorizzato in un sistema costituisce un reato. Se siete interessati a studiare la sicurezza della vostra postazione di lavoro o della rete di cui fate parte, chiedete preventivamente l'autorizzazione al responsabile della sicurezza del singolo ufficio/servizio/unità operativa. Non

utilizzate senza autorizzazione software che possa creare problemi di sicurezza o danneggiare la rete, come port scanner, security scanner, network monitor, network flooder, fabbriche di virus o di worm.

23. ***Segnalare tempestivamente all'amministratore di sistema qualsiasi variazione del comportamento della propria postazione di lavoro*** perché può essere il sintomo di un attacco in corso.

24. ***Segnalare comportamenti che possano far pensare a tentativi di ridurre la sicurezza del sistema informativo***. Ad esempio segnalate al responsabile della sicurezza dell' ufficio/servizio/unità operativa se un altro utente insiste per avere accesso ai vostri dati o per conoscere la vostra password o per poter lavorare alla vostra postazione di lavoro. Analogamente, non fidatevi e segnalate telefonate o messaggi che sembrano provenire da un sistema e vi chiedono di fare operazioni strane sul vostro computer (ad esempio, cambiare subito la password con una datavi al telefono o nel corpo del messaggio).