PRESCRIZIONI PER IL TRATTAMENTO DEI DATI DA PARTE DEI RESPONSABILI E DEGLI INCARICATI

1. Sicurezza.

1) I dati ed i sistemi di supporto (hardware, software e supporti di memorizzazione) devono essere adeguatamente protetti contro il rischio di: intrusione fisica, furto, incendio, allagamento, eccessiva umidità ed altri rischi di origine fisica. In genere, l'accesso fisico ai sistemi deve essere ristretto solo alle persone autorizzate, e va sempre controllato.
2) È vietato utilizzare strumenti di memorizzazione (anche materiale cartaceo) per trasportare dati da e verso l'esterno dell' Azienda. Nella presenza di tale necessità gli utenti sono tenuti a chiedere l'autorizzazione al responsabile di riferimento, il quale può autorizzare l'incaricato a portare i supporti al di fuori dell'Ufficio prendendo nota del nominativo dell'incaricato autorizzato, dei supporti trattati e della destinazione degli stessi. Al termine del trattamento, i supporti devono essere riposti negli archivi all'interno dell'Ufficio di provenienza.
3) L'utilizzo delle procedure informatizzate è consentito agli Incaricati del trattamento ai quali viene assegnata, da parte del Responsabile del trattamento, specifica parola chiave (password).
4) La parola chiave è segreta e non deve essere esposta né essere facilmente individuabile; è in possesso ed uso esclusivo del Responsabile del trattamento o dell'Incaricato quindi; deve essere composta di almeno 8 caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; tale password deve essere modificata al primo utilizzo e sostituita almeno ogni 6 mesi, ogni 3 in caso di trattamento di dati sensibili.
5) Ogni Responsabile del trattamento dati avrà cura di archiviare copia delle password (in busta chiusa).
6) Al termine del proprio lavoro o in caso di allontanamento temporaneo dal proprio posto l'Incaricato dovrà disattivare il Personal Computer o il terminale in modo che nessuno possa accedervi.
7) Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione: in caso di modifica occorre avvisare con comunicazione scritta il Servizio dal quale la parola chiave è stata assegnata.
8) L'utente è tenuto a cambiare la password al primo utilizzo.
9) A propria tutela va assolutamente evitato di comunicare la password (incluse quelle già utilizzate in passato) a terzi, escluso naturalmente il personale autorizzato.
10) Tutti i files contenenti dati sensibili e/o personali devono essere inseriti nelle cartelle del proprio profilo (ad esempio la cartella Documenti) poiché sono le uniche che, nell' attuale implementazione del dominio, siano visibili solo dopo l'accesso al sistema operativo tramite credenziale di autorizzazione.
11) I supporti informatici contenenti dati sensibili e giudiziari devono essere utilizzati per il tempo strettamente necessario alle operazioni di trattamento.
12) Gli archivi presenti nei Personal Computer collegati in rete devono essere condivisi solo con gli Incaricati che hanno titolo ad accedervi.
13) I supporti magnetici esterni (nastri magnetici, floppy disk, etc) devono essere custoditi da ciascun Incaricato in modo tale da evitarne la visione, sottrazione, copiatura o distruzione non autorizzate.
14) In caso di dismissione, i supporti magnetici che contengono dati sensibili o giudiziari devono essere distrutti o resi inutilizzabili.
15) I locali nei quali vengono trattati dati personali con strumenti elettronici/automatizzati vanno chiusi a chiave al termine dell'orario di lavoro per impedire intrusioni o asportazioni di apparecchiature o di supporti magnetici esterni compatibilmente con le prescrizioni in materia di sicurezza dei luoghi di lavoro.
16) .Il trattamento dei dati genetici deve avvenire in locali protetti e accessibili ai soli Incaricati o ai soggetti preventivamente autorizzati ad accedervi. Il trasporto dei dati all'esterno dei locali riservati al trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti. Il trasferimento dei dati deve essere cifrato.
17) La comunicazione tra Incaricati dei dati personali/sensibili via internet può avvenire esclusivamente con l' utilizzo di VPN con criptazione dei dati stessi, o tramite connessione intranet su rete dedicata ed ad uso esclusivo dell'Azienda ULSS 6 Vicenza.
18) Nei casi in cui non si utilizzi un sistema centralizzato di controllo della vulnerabilità degli strumenti elettronici (aggiornamento antivirus tramite rete ospedaliera), devono essere aggiornati almeno annualmente i sistemi antivirus installati negli elaboratori elettronici(semestralmente in caso di trattamento di dati sensibili).

2. Installazione di Software, Hardware e/o supporti di memorizzazione

1) Tutti gli utenti si impegnano ad evitare azioni tese a superare le protezioni applicate ai sistemi. Le azioni di riparazione e configurazione sono a carico dei responsabili dei sistemi informativi o del referente esterno a cui compete l'assistenza.
2) Tutte le applicazioni sviluppate internamente sono di proprietà Aziendale, e come tale devono essere accessibili per verifica da parte dei responsabili dei servizi IT.

3. Virus

1) I virus rappresentano una delle più grosse minacce per i dati aziendali; di norma, peraltro, il software antivirus è in grado di prevenire le intrusioni e di eliminarle quando si verificano.
2) È necessario che il software antivirus sia sempre aggiornato ed in funzione. A tale scopo l'utente è tenuto a verificare che il software sia sempre attivo. In nessun caso il software antivirus deve essere disattivato.
3) Per abbassare il rischio di immissione di virus nei sistemi, si richiede che gli utenti seguano le seguenti linee di sicurezza:
    - Tutti i dati provenienti da fonti non certificate (es. supporti magnetici esterni, floppy, CD, DVD, nastri) devono essere controllati per la presenza di virus. A tale scopo si richiede di limitare al minimo indispensabile l'utilizzo di files provenienti da supporti esterni;
    - Qualsiasi tipologia di software gratuito (freeware, shareware) trovato in rete o allegato a riviste o libri non va mai installato;
    - Tutti i files allegati a posta elettronica vanno controllati per la presenza di virus, o nel caso di link a fonti non conosciute o sospette. Nel caso di messaggi di posta, contenenti files o link, provenissero da fonti sconosciute o comunque inaspettate, questi vanno distrutti;
    - E' consentito l'utilizzo di Internet solamente per la ricerca e la visione di siti con fini istituzionali o per attività strettamente pertinenti al servizio;
    - Non vanno mai prelevati files da siti Internet ritenuti incerti o insicuri.

*4. Posta elettronica, Web, Internet e Intrane***t**

1) Ogni utente è responsabile dell'uso dell'identificativo di posta elettronica assegnato e può farne uso solo per motivi professionali legati all'attività aziendale.
2) E' fatto esplicito divieto di utilizzare la posta elettronica aziendale per la partecipazione a dibattiti, forum, mailing list che non siano legati al business aziendale.
3) La posta elettronica ricevuta attraverso spamming (email indesiderate, promozionali o commerciali) va immediatamente eliminata senza effettuarne la lettura, così come non devono essere aperti gli allegati di posta elettronica di provenienza ignota o comunque incerta;
4) L'accesso ai servizi resi disponibili dalla rete è consentito solo per esigenze professionali.

5. Backup dei dati (copia di salvataggio dei dati)

1) Con periodicità almeno settimanale dovrà effettuarsi un back-up (copia), elettronica o cartacea, di tutti quei documenti che contengono dati personali.
2) Tali copie dovranno essere conservate in locali distinti, chiusi a chiave, non accessibili a terzi e con caratteristiche tali da garantire l'integrità dei dati;
3) Tale attività è a carico dell' utente incaricato del trattamento se non diversamente disposto dai servizi informatici attraverso dispositivi centralizzati.

6. Il reporting degli incidenti

Tutti gli incidenti legati alla sicurezza devono essere comunicati tempestivamente al Responsabile del trattamenti dati.

7. Verifiche, deterrenti e sanzioni

Il Servizio per l'Informatica generale ha la facoltà di adottare soluzioni di monitoraggio e di sorveglianza di tutto il traffico da e verso Internet; i dati ottenuti non sono nominativi, tuttavia permettono di evidenziare un uso scorretto della rete di dati che sarà contestato in termini disciplinari.

8. Aggiornamento delle politiche

Il presente regolamento viene aggiornato con scadenza almeno annuale.Tutti gli utenti del sistema informativo possono proporre modifiche ed integrazioni.