Informazioni Sicurezza Informatica

1. Adempimenti per tutti gli elaboratori:

Si applicano le seguenti disposizioni a tutti gli elaboratori, presso i quali risiedono le banche-dati contenenti informazioni di tipo personale e/o di tipo sensibile:

1.1 attribuzione di una "parola chiave" (password) utile per l'accesso all'elaboratore.

La password è necessaria per avere accesso all'elaboratore, e quindi ai dati in esso contenuti. La password dovrà avere una **lunghezza minima di 8 caratteri alfanumerici** (lettere e numeri), si sconsiglia l'uso di date di nascita, matrimonio, nomi di figli o della moglie, in ogni caso si sconsiglia di utilizzare informazioni facilmente rilevabili da chi in malafede volesse accedere al personal computer.

Un esempio di password "corretta": **FH7J6IW9**

E' preferibile che oltre alla password da attribuire all'elaboratore, ne venga applicata una ulteriore alle banche-dati in esso contenute, ciò è facilitato dagli applicativi in uso comune (Microsoft WinWord ed Access).
La password dovrà essere modificata autonomamente ogni 6 (sei) mesi.
Inoltre, l'assegnazione dovrà essere **univoca** e cioè non assegnabile ad altre persone, neanche in tempi diversi. Quindi, per l'accesso all'elaboratore non è possibile assegnare una parola chiave uguale per più soggetti autorizzati, ed inoltre si suggerisce una custodia "personale" della stessa (nella borsa, nella propria agenda, ecc.), al fine di evitare un facile reperimento da parte di terzi.
Il responsabile di ogni U.O. provvederà a trasmettere al Responsabile della Sicurezza di ciascun Settore, copia dell'elenco contenente tutte le passwords ed i nominativi che detengono la custodia delle stesse, provvedendo all'aggiornamento di tale elenco ogni 6 (sei) mesi.
Inoltre occorre prevedere l'immediata disattivazione delle passwords sia in caso di perdita della qualità all'accesso, da parte del soggetto, che di mancato utilizzo per oltre un semestre, al fine di garantire un costante controllo sui codici, ed evitare che quelli non più in uso possano essere utilizzati per accedere ai dati personali.
Non è consentita la cessione dell'uso della propria "parola chiave" al collega, neanche in forma temporanea. Nel caso di un solo elaboratore condiviso da più persone, allora le stesse saranno tutte a conoscenza dell'unica chiave di accesso, e la modifica di quest'ultima dovrà avvenire con cadenza trimestrale.
Nel caso di computers collegati in rete locale, la responsabilità della custodia delle password di ogni utilizzatore sarà a cura dell'amministratore di sistema, cioè colui che sovrintende alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e ne consente l'utilizzazione.

1.2 Redazione apposito elenco dei soggetti autorizzati all'uso delle passwords dell'ufficio, tale elenco va aggiornato ogni 6 (sei) mesi e comunicato al Responsabile della

Sicurezza. Gli stessi soggetti sono preposti alla custodia delle passwords ed hanno accesso alle informazioni che concernono le medesime.
Nel caso di trattamento di dati "sensibili" e/o "giudiziari", l'accesso agli elaboratori per effettuare le operazioni di trattamento è determinato sulla base di autorizzazioni assegnate dal Dirigente del Dipartimento di appartenenza, singolarmente o per gruppi di lavoro, agli incaricati del trattamento o della manutenzione. Così come occorre controllare l'accesso agli archivi ed identificare e registrare i soggetti che vi vengono ammessi dopo l'orario di chiusura degli archivi stessi.
L'autorizzazione all'accesso dovrà essere limitata ai soli dati la cui conoscenza è necessaria e sufficiente per lo svolgimento delle operazioni di trattamento o di manutenzione.
La validità delle richieste di accesso ai dati personali è verificata prima di consentire l'accesso stesso.
Le suddette misure non si applicano al trattamento dei dati personali di cui è consentita la diffusione.

1.3 Reimpiego dei supporti magnetici (floppy-disk, cartridge, nastri, ecc.):

In tutti i casi di reimpiego di supporti magnetici, nei quali in precedenza siano state memorizzate informazioni di dati personali e/o sensibili, si suggerisce prima del reimpiego la formattazione a basso livello dello stesso supporto magnetico, al fine di non rendere tecnicamente ed in alcun modo recuperabili le informazioni memorizzate precedentemente. In caso contrario o nell'impossibilità di tale attività, se ne suggerisce la distruzione del supporto magnetico.

Esempio di formattazione a basso livello di un floppy-disk:
digitare quando appare il prompt C:>

format A: ↵ (premere **Invio**)

1.4 Utilizzo di elaboratori collegati ad Internet tramite modem:

SI suggerisce al fine di garantire l'integrità delle banche-dati residenti in personal computer, che vengono utilizzati anche per il collegamento alla rete Internet, di provvedere allo spegnimento del modem (nel caso trattasi di modem esterno) alla fine del suo utilizzo. Questo al fine di evitare eventuali intrusioni non autorizzate da parte di soggetti terzi dall'esterno.