

Check list

referita all'ALLEGATO B - parte prima - DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA - (Articoli da 33 a 36 del codice)

Trattamenti con strumenti elettronici

Modalità tecniche da adottare a cura del titolare, del responsabile (ove designato) e dell'incaricato, in caso di trattamento con strumenti elettronici:

Sistema di autenticazione informatica

1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.

| | |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| 1. Gli Utenti sono dotati delle credenziali di autenticazione che consentano il loro "login" al sistema ? | |
| 1.1 Il "login" al sistema consente all'utente di accedere indistintamente a tutte le informazioni presenti sul sistema informatico? In caso di risposta positiva passare alla domanda 2. | |
| 1.2 In caso si disponga di accessi personalizzati, l'ambito di utilizzo delle risorse per ciascun utente è stato definito e/o comunicato per iscritto all'utente ? | |
| 2. Le credenziali di autenticazione sono composte da "user-name" (nome utente) e da "password" (parola chiave per l'accesso)? In caso negativo passare alla 2.4. | |
| 2.2 Gli utenti dispongono di parole chiave univoche, a loro solamente riservate e da loro solamente riconosciute? | |
| 2.3 Gli utenti possono scambiarsi user-name e password" tra loro ? | |
| 2.4 Le credenziali di autenticazione sono state sostituite da altri sistemi (ad esempio riconoscimento biometrico dell'incaricato con codice identificativo o con parola chiave) ? | |
| 3. Le credenziali di autenticazione sono univocamente assegnate o associate individualmente ad un solo utente ? | |
| 4. Sono state impartite per iscritto agli incaricati le raccomandazioni di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato ? | |
| 5. Le password sono composte da almeno otto caratteri ? | |
| 5.1 Nel caso in cui lo strumento elettronico non lo permetta, le password sono composte da un numero di caratteri pari al massimo consentito ? | |
| 5.2 Gli utenti sono stati interdetti dall'utilizzo di codici identificativi agevolmente riconducibili all'incaricato | |
| 5.3 Gli utenti sono stati interdetti dall'utilizzo di codici identificativi contenenti riferimenti di tipo personale tipo data di nascita, nome dell'animale domestico ? | |
| 5.4 Le password sono state modificate dopo il primo utilizzo ? | |

| | |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| 5.5 Le password sono cambiate almeno ogni sei mesi ? (tre in presenza di dati sensibili) | |
| 6. Sono state adottate regole per il non utilizzo di codici di identificazione, laddove utilizzati, neppure in tempi diversi ? | |
| 7. E' prevista la disattivazione delle credenziali di autenticazione non utilizzate da almeno sei mesi ? | |
| 7.1 Sono previste speciali autorizzazioni per le credenziali eventualmente utilizzate per soli scopi di gestione tecnica ? | |
| 8 E' prevista la procedura per disabilitare le credenziali di autenticazione in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali ? | |
| 9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento ? | |
| 10. Nei casi di impedimento e/o prolungata assenza dell'incaricato oppure di indispensabile e indifferibile intervento per necessità di operatività e di sicurezza del sistema sono state impartite idonee e preventive disposizioni scritte per individuare le modalità con le quali il titolare può disporre dei dati e degli strumenti elettronici ? | |
| 10.1 Esiste una copia delle credenziali di autenticazione ? | |
| 10.2 Le copie delle credenziali sono state affidate per iscritto ad un custode/responsabile ? | |
| 10.3 I responsabili della custodia delle password sono stati avvisati con istruzione scritta del loro dovere di informare tempestivamente l'incaricato degli eventuali interventi effettuati ? | |
| 11. Gli incaricati al trattamento sono stati informati che le disposizioni sul sistema di autenticazione (di cui ai precedenti punti) e quelle sul sistema di autorizzazione non è applicabile ai trattamenti dei dati personali destinati alla diffusione ? | |

Sistema di autorizzazione

| | |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| 12. Il sistema di autorizzazione, atto a verificare le credenziali, discrimina gli ambiti di autorizzazioni in base ai profili di autorizzazione prestabiliti ? | |
| 13 I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento ? | |
| 14. E' stato adottato un piano delle verifiche periodiche (almeno annuali) per la verifica della sussistenza delle condizioni per la conservazione dei profili di autorizzazione ? | |

Altre misure di sicurezza

| | |
|-----------------------------------------------------------------------------------------------------------------------------|--|
| 15. Sono stati eseguiti raggruppamenti per classi omogenee di incarico ? Se non sono stati definiti passare alla numero 16. | |
| 15.2 L'accesso alla classe omogenea è regolamentato ? | |
| 15.3 L'accesso alla classe omogenea è conforme al profilo di autorizzazione ? | |

| | |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| 15.4 Classi omogenee e profili di autorizzazione vengono periodicamente sottoposti a verifica (almeno annuale) ? | |
| 16. I dati personali sono protetti contro il rischio di intrusione (Art. 615-quinquies del codice penale) ? | |
| 16.1 Si dispone di antivirus aggiornato settimanalmente ? (anche se la legge dice sei mesi!!!) | |
| 16.2 Si dispone di Firewall (software e/o Hardware) ? | |
| 16.3 Si dispone di connessione internet con IP stabile ? | |
| 16.4 Si dispone di rete Wireless (senza fili / ad onde radio) | |
| 16.5 Si dispone di protocollo di autenticazione Wireless ? | |
| 17. I programmi per elaboratore che consentono di allontanare il rischio intrusione di cui all'Art. 615-quinquies del codice penale sono aggiornati almeno ogni sei mesi (tre se si trattano dati sensibili) ? | |
| 18. Le copie vengono eseguite ogni settimana ? | |
| 18.1 Le copie sono depositate in cassaforte ignifuga ? | |
| 18.2 Esiste un registro delle copie ? | |
| 18.3 E' stato definito un incaricato ed un apposito piano di ripristino da copia in caso di perdita totale o parziale di dati? | |