ALLEGATO B
Trattazione informatica di informazioni a carattere "controllate e/o sensibili”

Per trattare informazioni e dati a carattere “controllate e/o sensibili” tramite un sistema informatico:

• Il legale rappresentante - o altro soggetto, socio o dipendente opportunamente designato dal legale rappresentante - assume la veste di amministratore di sistema ed esercita tale funzione secondo la normativa in materia di seguito riportata.
• L'amministratore di sistema è responsabile degli aspetti tecnici e di sicurezza del sistema destinato a trattare informazioni a carattere "controllate e/o sensibili".
• Quando le informazioni a carattere "controllate e/o sensibili" sono trattate mediante sistemi informatici, l'amministratore di sistema deve assicurare che siano applicate le seguenti misure di sicurezza:

1) Il sistema informatico deve essere isolato. A tal fine si deve:

• rimuovere, dove possibile, la scheda hardware per il collegamento in rete o provvedere alla rimozione dei driver relativi, premessa l'assenza di alcun cavo collegato alla medesima;
• rimuovere, dove possibile, la scheda hardware per il collegamento in rete a mezzo wireless (Wi-Fi, 3G, Bluetooth, ecc.) o provvedere alla rimozione dei driver relativi;
• disabilitare l'utilizzo delle porte USB o comunque limitarne l'utilizzo alla sola utenza di amministratore di sistema;

2) dotare il BIOS di password al fine di evitare la possibilità di avvio da CD/DVD o memorie rimovibili USB;

3) installare un sistema operativo in possesso di certificazione Common Criteria di livello EAL3 o superiore, seguendo le indicazioni riportate nel documento di Security Target della specifica versione e delle guide di installazione e configurazione cui esso faccia riferimento:

4) installare un sistema Antivirus, possibilmente in versione certificata Common Criteria per il sistema operativo prescelto;

5) abilitare le funzioni di controllo accessi e configurare utenze nominative (non sono ammesse utenze di gruppo) con password non banali, di lunghezza non inferiore agli 11 caratteri e contenenti almeno tre dei seguenti criteri di sicurezza:

• almeno un carattere maiuscolo;
• almeno un carattere minuscolo;
• almeno un carattere speciale consentito dal sistema operativo (es. £,$);
• almeno un carattere numerico;

6) le password dovranno essere modificate dagli utenti dopo il primo accesso;

7) deve essere presente una sola utenza con il possesso dei diritti di amministrazione;

8) abilitare lo screen saver dopo massimo 5 minuti di inattività della postazione, con il ritorno alla schermata di ingresso al ripristino:

9) abilitare il sistema di log del sistema operativo;

10) abilitare il log delle stampe;

11) abilitare l'audit degli eventi sia per il caso di successo che per il caso di fallimento:

• controllo eventi accesso account;
• controllo eventi di accesso;
• controllo gestione degli account;
• controllo degli usi dei privilegi;
• controllo della modifica del criterio di controllo;

12) disabilitare il controllo tramite remote desktop;

13) non installare sistemi di remote desktop o ambienti di virtualizzazione;

14) nei casi in cui si renda necessario l'impiego di software come Application Server, provvedere a installare prodotti in possesso di certificazione Common Criteria di livello EAL3 o superiore, seguendo le indicazioni riportate nel documento di Security Target della specifica versione e delle guide di installazione e configurazione cui esso faccia riferimento;

15) nei casi di sviluppo di prototipi di applicazioni web che prevedano la presenza di un controllo accessi, questo deve essere connesso con l'archivio utenti del sistema operativo (Active Directory, ecc.) e comunque non può determinare una grana più fine rispetto alle utenze configurate su sistema operativo;

16) provvedere a effettuare gli aggiornamenti periodici del sistema antivirus e del sistema operativo in modalità off-line, solo dopo aver verificato la correttezza delle misure applicate e la corrispondenza della firma degli aggiornamenti scaricati da repository ufficiali del brand fornitore del sistema stesso;

17) tutti i media a carattere “controllate e/o sensibili” in uso al sistema devono avere un numero identificativo;
18) non si possono produrre stampe. Eventuali bozze devono essere distrutte al termine dell'esigenza;

19) il sistema deve essere installato in un ambiente ad accesso controllato, o comunque custodito in apposito contenitore di sicurezza. Deve essere anche valutata la possibilità di dotare l'ambiente di sistemi anti-intrusione in grado di monitorare l'eventuale accesso non autorizzato al sistema;

20) tutti gli utenti devono essere opportunamente istruiti a cura dell'amministratore di sistema in merito alle procedure di sicurezza implementate;

21) a cessata esigenza è necessario assicurare l'attuazione delle più accurate procedure per la completa cancellazione delle informazioni a carattere “controllate e/o sensibili” memorizzate o elaborate. In particolare l'amministratore deve curare che:

• tutti i dischi rigidi presenti nel sistema siano sottoposti a una formattazione a basso livello e a quattro cicli completi di scrittura e cancellazione;
• il sistema operativo sia re-installato, assicurando che le nuove utenze non utilizzino username e password in uso alla precedente installazione;
• analoga procedura sia effettuata per i supporti di memorizzazione eventualmente presenti all'interno delle stampanti o di altre periferiche autorizzate;