Allegato C

(*articolo 9*)

Misure minime di sicurezza per la tutela delle informazioni

1. Trattamenti con l'ausilio di strumenti elettronici

a) Identificazione degli utenti e gestione delle identità digitali;

b) determinazione dei privilegi di accesso alle risorse da associare agli utenti e agli addetti o incaricati alla gestione o alla manutenzione;

c) implementazione di un sistema di autenticazione e autorizzazione degli utenti secondo i privilegi individuati al punto precedente;

d) protezione contro il software malevolo mediante l'impiego di *software antimalware* aggiornato

e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;

f) procedure di sicurezza per l'importazione e l'esportazione dei dati sui sistemi impiegati;

g) procedure per la gestione della configurazione dei sistemi impiegati;

h) procedure per la dismissione dei dispositivi di memorizzazione utilizzati sui sistemi impiegati;

i) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;

l) adozione di tecniche di cifratura.

2. Misure di sicurezza fisica e documentale

a) L'accesso alle informazioni è consentito sulla base del principio della necessità di conoscere (*need to know*);

b) deve essere individuata la figura di un responsabile incaricato della gestione delle informazioni, preferibilmente già in possesso di abilitazione di sicurezza ai sensi dell'articolo 42 della legge 3 agosto 2007, n. 124;

c) la documentazione deve essere custodita in un locale idoneo, appositamente individuato, che presenti un perimetro chiaramente delimitato e sia dotato di misure di protezione minime tali da consentire l'accesso alle sole persone autorizzate, ovvero in armadi di sicurezza con procedura di tracciamento delle chiavi in uso;

d) la documentazione deve essere registrata su appositi registri di protocollo;

e) la consultazione dei documenti deve avvenire sulla base del principio della necessità di conoscere (*need to know*) e deve essere tracciata su apposito registro;

f) la riproduzione dei documenti può avvenire solo previa autorizzazione del responsabile della gestione delle informazioni e deve essere registrata su apposito registro;

g) la documentazione deve essere spedita tramite corrieri.