Allegato n. 1 – Regole per l'adozione delle misure di sicurezza

Le misure di sicurezza che l'Istituto adotta, vengono valutate sulla base de rischio e del contesto ambientale, così come dettato dall'art. 32 del GDPR, il quale espressamente dispone "*Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio*

Si riportano, a titolo esemplificativo, le misure di sicurezza che l'Istituto intende implementare sulla base di specifici principi e regole per la loro applicabilità.

Misure	Regole / Principi da osservare
Presenza di un sistema di allarme	E' importante che l'Istituto si doti di impianto d'antifurto a tutela del patrimonio delle informazioni contenute al suo interno.
Custodia dei dati in armadi blindati e/o ignifughi	E' importante che gli uffici che trattano dati sensibili e giudiziari possano disporre di queste strutture per archiviare in modo consono tali informazioni.
Sistemi UPS e Generatori di corrente che garantiscano la continuità elettrica	Fondamentale a tutela delle attività soprattutto per gli strumenti elettronici. Da adottare necessariamente per tutti i server e per quei pc locali che non archiviano le informazioni sul server. Infatti questi ultimi non hanno delle procedure pianificate di backup e quindi è importante ridurre al minimo i rischi che gli sbalzi di tensione possono provocare sugli hard disk.
Digitazione password all'accensione del PC	Tutti i PC devono avere la password di Windows all'accensione del terminale, questo non vale solo come regola ma viene considerata una misura base di sicurezza.
Manutenzione programmata degli strumenti	Come tutte le macchine che si rispettano anche il sistema informativo va manutenzionato periodicamente sia attraverso l'aggiornamento dei suoi componenti sia con la pulizia periodica delle macchine stesse.
Utilizzo di un sistema firewall	Obbligatorio viste le forme di attacco sempre più intelligenti.

Presenza di un sistema di autenticazione delle credenziali per tutti gli accessi agli archivi elettronici	Si intende con questa misura l'adozione di un server di dominio che consenta l'autenticazione dell'utente.
Disattivazione delle credenziali di autenticazione nel caso di inutilizzo per 6 mesi	Spetta all'incaricato della custodia delle password disattivare le credenziali che hanno perso efficacia
Controllo degli accessi a siti internet non sicuri – Protezione della posta elettronica	É importante la conoscenza da parte degli operatori della navigazione in internet e dell'uso della posta elettronica. A questo proposito è stato introdotto il regolamento per l'uso del PC.
Utilizzo di un filtro anti-spam	All'interno dello spam (posta indesiderata) si annidano spesso dei fenomeni di illegalità informatica. È importante dotare l'Istituto di tale strumento
Utilizzo di un antivirus	Per quanto precedentemente detto, è importante la presenza di un antivirus in ogni posto di lavoro, considerata misura di sicurezza e ovviamente che sia aggiornato
Istruzioni in merito alla protezione dello strumento elettronico in caso di assenza temporanea durante le sessioni di lavoro	E' importante che l'operatore conosca il regolamento per quanto concerne l'assenza dal posto di lavoro con il PC acceso.
Disattivazione delle credenziali di autenticazione in caso di perdita di qualità dell'incarico	Spetta all'incaricato della custodia delle password disattivare le credenziali che hanno perso efficacia
Aggiornamento periodico, con cadenza almeno annuale, della lista degli incaricati e dei profili di autorizzazione	Tutte le persone che operano all'interno degli uffici devono essere autorizzate dal Titolare
Istruzioni in merito alla segretezza e alla custodia delle credenziali di autenticazione	Rientra nel concetto della formazione del personale
Aggiornamento periodico delle credenziali di autenticazione	Spetta all'incaricato della custodia delle password disattivare le credenziali che hanno perso efficacia
Procedure di verifica sull'operato degli incaricati	È un compito ispettivo che il Responsabile della sicurezza dei dati personali può demandare anche a società esterne

Formazione sugli aspetti principali della disciplina della privacy al momento dell'ingresso in servizio	Rientra nel concetto della formazione del personale
Formazione, periodica e in occasione di cambiamenti di mansioni o di introduzione di nuovi strumenti per il trattamento dei dati e la loro protezione	Rientra nel concetto della formazione del personale
Istruzioni finalizzate al controllo e alla custodia dei documenti contenenti dati personali per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento	Rientra nel concetto della formazione del personale
Adozione di procedure per le copie di sicurezza, la loro custodia ed il ripristino della disponibilità dei dati	Il backup dei dati trattati dagli uffici amministrativi essere metodico, non affidato alle singole volontà. E' per questo importante nominare l'Incaricato delle copie di sicurezza delle banche dati
Definizioni di responsabilità e sanzioni disciplinari	Rientra nel concetto della formazione del personale nonché è necessario integrare il codice di comportamento includendo sanzioni disciplinari nei casi in cui ci sia un comportamento difforme da quando indicato dal presente Regolamento
Formazione professionale	Rientra nel concetto della formazione del personale
Distruzione del cartaceo	È importante nel limite del possibile incentivare la distruzione del cartaceo rendendolo illeggibile usando dei comodi distruggi documenti. In assenza di tali strumenti, sarà cura del singolo dipendente provvedere alla distruzione manuale in modo che lo stesso non possa essere facilmente ricostruibile.
Per accedere sono attive le credenziali di autenticazione	Questa misura comporta, per gli uffici amministrativi, l'adozione di un server di dominio che consenta l'autenticazione dell'utente
Definizione di procedure per le copie di sicurezza, la loro custodia e il ripristino dei dati	Il salvataggio dei dati è fondamentale in qualsiasi organizzazione
I dati cartacei sono chiusi in un armadio	Ogni documento deve essere possibilmente chiuso in un armadio. Qualora questo non possa essere possibile, sicuramente che possano essere chiusi i dati sensibili e quelli giudiziari