Prot.n.3572 Barletta, 30/09/2016

**AL Sig. LAMACCHIA Vito**

**Titolare ditta ANYSYSTEM di LAMACCHIA VITO**

**SEDE**

**OGGETTO: incarico per il Responsabile della Sicurezza Informatica**

D.Lgs. 30 giugno 2003, n. 196 “Codice in materia di protezione dei dati personali”;

“Allegato B”: “Disciplinare tecnico in materia di misure minime di sicurezza”

IL DIRIGENTE SCOLASTICO

**VISTO** il D.Lgs 30 giugno 2003, n. 196 “Codice in materia di protezione dei dati personali” e l’Allegato B: “Disciplinare tecnico in materia di misure minime di sicurezza”;

PREMESSO CHE

* ai sensi dell’art. 28 del Codice, Titolare del trattamento dei dati personali trattati da questo ente è l’Istituto stesso, di cui il sottoscritto è Legale Rappresentante pro-tempore;
* il Titolare, ai sensi dell’art. 29 del Codice, può designare uno o più Responsabili del trattamento tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia privacy;
* ai sensi dell’art. 30 del Codice, è necessario procedere alla nomina di “Incaricati del trattamento dei dati personali” e ciò può avvenire anche mediante l’individuazione di unità organizzative alle quali i singoli dipendenti sono assegnati;

DESIGNA

il Sig. **LAMACCHIA Vito** quale

RESPONSABILE DELLA SICUREZZA INFORMATICA

Le affidiamo:

* l’organizzazione, gestione e supervisione di tutte le operazioni di sicurezza dei dati personali che il nostro istituto effettua nelle proprie sedi;
* l’organizzazione, gestione e supervisione di tutte le operazioni di sicurezza dei dati personali dei clienti e/o fornitori – persone fisiche della nostra organizzazione.

In tale ambito, sarà Suo compito:

1. garantire che tutte le misure minime di sicurezza riguardanti i dati personali siano applicate secondo le misure minime di sicurezza riportate nell’Allegato B del Codice Unico;
2. sorvegliare che il trattamento sia effettuato nei termini e nei modi stabiliti dal Codice in materia di dati personali;
3. dare le istruzioni adeguate agli incaricati del trattamento effettuato con strumenti elettronici;
4. verificare e attivare le credenziali di autenticazione agli incaricati del trattamento, su indicazione del Responsabile del trattamento dati, per tutti i trattamenti effettuati con strumenti informatici;
5. verificare e revocare tutte le credenziali non utilizzate in caso di perdita della qualità che consentiva all’incaricato l’accesso ai dati personali;
6. verificare e revocare le credenziali per l’accesso ai dati degli incaricati del trattamento dati nel caso di mancato utilizzo per oltre 6 (sei) mesi;
7. verificare che siano istruiti gli incaricati del trattamento sull’uso delle parole chiave, e sulle caratteristiche che debbono avere, e sulle modalità per la loro modifica in autonomia;
8. verificare che siano definite le politiche da adottare per la protezione dei sistemi contro virus informatici e verificarne l’efficacia con cadenza almeno semestrale;
9. proteggere gli elaboratori dal rischio di intrusione (violazione del sistema da parte di “hackers”);
10. verificare che siano redatti ed aggiornati ad ogni variazione l’elenco dei sistemi di elaborazione;
11. individuare, nominare e incaricare per iscritto, uno o più responsabili alla manutenzione informatica;
12. individuare, nominare e incaricare per iscritto, uno o più responsabili all’amministrazione del sistema informatico e delle credenziali;
13. individuare, nominare e incaricare per iscritto, uno o più Incaricati delle copie di sicurezza delle banche dati;
14. individuare, nominare e incaricare per iscritto, uno o più Incaricati della custodia delle copie delle credenziali.

Sarà inoltre Sua cura organizzare le operazioni di trattamento affinché esse siano effettuate nel rispetto delle disposizioni di legge, con particolare riferimento alle norme relative alle informazioni ed al consenso degli interessati, all’autorizzazione del Garante ed alla adozione delle misure di sicurezza.

Provvederà ad organizzare le mansioni in modo tale, che agli interessati del trattamento venga data pronta soddisfazione nell’esercizio dei loro diritti, di cui all’articolo 7 del D.Lgs. 196/2003 (*Diritto di accesso ai dati personali ed altri diritti*), e ad avvisare immediatamente il titolare del nostro istituto di ogni richiesta, ordine o attività di controllo da parte del Garante o dell’Autorità Giudiziaria, ai sensi degli articoli 152 e da 157 a 160 D.Lgs. 196/2003.

Sarà Suo compito riferire periodicamente, ed in ogni caso con cadenza mensile, al titolare del nostro istituto sullo svolgimento dei Suoi compiti, dandogli inoltre piena collaborazione nello svolgimento delle verifiche periodiche circa il rispetto delle disposizioni di legge e l'adeguatezza delle misure di sicurezza adottate

Si precisano gli atti che dovranno intervenire e che Lei dovrà curare e regolamentare a seguito dell'emanazione dell’Allegato B al Codice Unico.

A seguito dell'emanazione del predetto Regolamento recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali, occorrerà approntare almeno le misure di sicurezza ivi previste.

Le ricordiamo che l’Allegato B del Codice Unico prevede particolari regole alle quali ogni incaricato dovrà attenersi nel trattamento dei dati personali medesimi; regole che vengono riportate nel seguente Allegato “TRATTAMENTO DEI DATI PERSONALI CON STRUMENTI DIVERSI DA QUELLI ELETTRONICI O COMUNQUE AUTOMATIZZATI” e che dovranno da Lei essere osservate.

**Timbro e Firma del Titolare del trattamento**

**IL DIRIGENTE SCOLASTICO**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Il *Responsabile della Sicurezza Informatica* dichiara di essere a conoscenza di quanto stabilito dal D.Lgs. 30 giugno 2003 n. 196 e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

Il *Responsabile della Sicurezza Informatica* dichiara che svolgerà l’incarico in osservanza ed ottemperando alle suddette direttive ed alle norme previste nel D.Lgs. 30 giugno 2003 n. 196.

L'incaricato del Trattamento dichiara di essere a conoscenza di quanto stabilito dall’Allegato B del Codice Unico e si impegna, nel trattamento dei dati personali ai quali è stato autorizzato ad accedere, ad attenersi alle regole qui indicate comprese quelle di cui all’Allegato “TRATTAMENTO DEI DATI PERSONALI CON STRUMENTI DIVERSI DA QUELLI ELETTRONICI O COMUNQUE AUTOMATIZZATI”.

**Il Responsabile della sicurezza informatica**

**(per accettazione delle regole qui contenute)**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**ALLEGATO**

**TRATTAMENTO DEI DATI PERSONALI CON STRUMENTI DIVERSI DA QUELLI ELETTRONICI O COMUNQUE AUTOMATIZZATI**

Per il trattamento di dati personali, effettuato con strumenti diversi da quelli elettronici o comunque automatizzati, èrichiesta l'osservanza almeno delle seguenti modalità:

*Art. 27. Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l’intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell’ambito dell’aggiornamento periodico con cadenza almeno annuale dell’individuazione dell’ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.*

Art. 28. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

*Art. 29. L’accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l’orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.*

**TRATTAMENTO DEI DATI PERSONALI CON STRUMENTI ELETTRONICI O COMUNQUE AUTOMATIZZATI**

**Trattamento dei dati personali *-*** Per il Trattamento dei dati personali effettuato con strumenti elettronici o comunque con strumenti automatizzati occorre prevedere, anteriormente all'inizio dei trattamento, almeno le seguenti misure:

Art. 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.

Art. 2. Le credenziali di autenticazione consistono in un codice per l’identificazione dell’incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell’incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell’incaricato, eventualmente associata a un codice identificativo o a una parola chiave.

Art. 3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l’autenticazione.

Art. 4. Con le istruzioni impartite agli incaricati è prescritto 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.

Art. 5. La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all’incaricato ed è modificata da quest’ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.

Art. 6. Il codice per l’identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.

*Art. 7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.*

*Art. 8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all’incaricato l’accesso ai dati personali.*

*Art. 9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.*

*Art. 10. Quando l’accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l’autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell’incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l’incaricato dell’intervento effettuato.*

*Art. 11. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.*

*Art. 15. Nell’ambito dell’aggiornamento periodico con cadenza almeno annuale dell’individuazione dell’ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.*

*Art. 16. I dati personali sono protetti contro il rischio di intrusione e dell’azione di programmi di cui all’art. 615-quinquies del codice penale, mediante l’attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale****.***

*Art. 17. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l’aggiornamento è almeno semestrale.*

*Art. 18. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.*

**E le seguenti autorizzazioni**:

Art. 12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.

Art. 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.

Art. 14. Periodicamente, e comunque almeno annualmente**,** è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

**Trattamento dei dati sensibili e giudiziari *-*** Per il Trattamento dei dati sensibili e giudiziari effettuato con strumenti elettronici o comunque con strumenti automatizzati occorre prevedere, anteriormente all'inizio dei trattamento, almeno le seguenti misure:

*Art. 20. I dati sensibili o giudiziari sono protetti contro l’accesso abusivo, di cui all’art. 615-ter del codice penale, mediante l’utilizzo di idonei strumenti elettronici.*

*Art. 21. Sono impartite istruzioni organizzative e tecniche per la custodia e l’uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.*

*Art. 22. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.*

*Art. 23. Sono adottate idonee misure per garantire il ripristino dell’accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.*

*Art. 24. Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all’articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all’identità genetica sono trattati esclusivamente all’interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all’esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.*

**Controlli** - Lo scrivente, TITOLARE, si riserva, anche tramite verifiche periodiche, di vigilare sulla puntuale osservanza delle disposizioni di legge sul trattamento dei dati stessi e sul rispetto delle proprie istruzioni in seguito indicate. IL *RESPONSABILE* dovrà consentire al *TITOLARE*, dandogli piena collaborazione, periodiche verifiche circa l'adeguatezza delle misure di sicurezza adottate e il rispetto della legge.

##### CRITERI GENERALI

I dati personali oggetto di trattamento devono comunque essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Il Dirigente Scolastico

prof.ssa *Rosa Carlucci*

Firma autografa sostituita a mezzo stampa ai sensi dell’art. 3, comma 2 del decreto legislativo n. 39/1993