Ministero Istruzione, Università e Ricerca

# LICEO SCIENTIFICO STATALE

*"Leonardo da Vinci"*

Via Zaccaria Pinto, 1 – 84078 Vallo della Lucania (SA) Aut. 75
Tel. 0974.4572 Fax: 0974.719487
c.m. SAPS10000T – e-mail ministeriale: SAPS10000T@istruzione.it
c.f. 84000540652 – e-mail: liceoscientificov@tiscali.it

2007-2013 Con l'Europa investiamo nel vostro futuro!

UNIONE EUROPEA

Prot. n. 4898 /A25c Vallo Della Lucania, 01/12/2012

**IL DIRIGENTE SCOLASTICO**

visto l'art. 29 del D. L.vo 30 giugno 2003, n. 196;

visto il D.M. n. 305 del 7 dicembre 2006, recante il Regolamento Ministeriale in materia di dati sensibili e giudiziari;

considerato che sussistono i requisiti di esperienza, capacità e affidabilità di cui all'art. 29 comma 2 del D. L.vo 30 giugno 2003, n. 196,

**DESIGNA**

il Sig. **DONNIANNI WALTER**, nato a **VALLO DELLA LUCANIA (SA)** il **29/05/1970** , alla funzione di **responsabile del trattamento** di dati personali per le seguenti aree ***Trattamento dati servizi di segreteria B1+B3+B4+ B7***.

In tale qualità il Sig. **DONNIANNI WALTER** è tenuto al rispetto delle disposizioni di legge ed in particolare:

- dovrà osservare il D. L.vo 30 giugno 2003 n. 196 e le altre disposizioni e regolamenti in materia di riservatezza delle persone osservando i principi di liceità e correttezza;
- dovrà censire i trattamenti di dati personali;
- individuare gli incaricati del trattamento e impartire le istruzioni necessarie per un corretto, lecito, sicuro trattamento;
- attuare gli obblighi di informativa nei confronti degli interessati;
- garantire all'interessato l'effettivo esercizio dei diritti previsti dall'art. 7 del D.L.vo n. 196/2003;
- collaborare per l'attuazione delle prescrizioni del garante;
- predisporre e aggiornare un sistema di sicurezza idoneo a rispettare le prescrizioni degli artt. da 31 a 36 e allegato B del D. L.vo n. 196/2003 e di ogni altra disposizione in materia nonché adeguare il sistema alle future norme regolamentari in materia di sicurezza;
- elaborare una relazione trimestrale sullo stato degli adempimenti previsti dal D. L.vo n. 196/2003.

L'INCARICATO

IL DIRIGENTE SCOLASTICO
Prof. Antonio Iannuzzelli

LICEO SCIENTIFICO STATALE
Leonardo da Vinci

Via Zaccaria Pinto, 1
84078 *Vallo della Lucania* (SA)
Aut. 75

c.m. SAPS10000T
c.f. 84000540652

☎ 0974.4572
🖷 0974.719487
✉ SAPS10000T@istruzione.it
(ministeriale)
✉ liceoscientificov@tiscali.it

FESR
Unione Europea
FONDI STRUTTURALI EUROPEI
PON 2007-2013
MIUR
COMPETENZE PER LO SVILUPPO (FSE) - AMBIENTI PER L' APPRENDIMENTO (FESR)

**Prot.n.4926 A/25c** **Vallo,li 01/12/2012**

# ATTO DI NOMINA DELL'AMMINISTRATORE DI SISTEMA
## D.Lgs. 196 del 30 giugno 2003

**Il Liceo Scientifico "L.Da Vinci" di Vallo della Lucania (SA)** nella persona del ***Dirigente Prof. Antonio Iannuzzelli*** in qualità di titolare del trattamento dei dati personali da esso operato, ai sensi e per gli effetti del D. Lgs. 196 del 30 giugno 2003 con il presente atto

## NOMINA

## AMMINISTRATORE DI SISTEMA

il Sig.**DONNIANNI WALTER**
nato il **29/5/1970** a ***VALLO DELLA LUCANIA(SA)***
Cod. Fiscale**DNNWTR70E29L628H**
e residente in **VALLO DELLA LUCANIA (SA) – fraz. Pattano - Cap 84078**
alla via **VELIA** n.civico **10**

**L' Amministratore di Sistema ha i seguenti compiti:**

- sovrintende alle risorse del sistema operativo di base dati e ne consente l'utilizzazione;
- vigila sul corretto funzionamento di tutti i componenti del sistema informatico, per evitare problemi di perdita o danneggiamento di dati personali;
- verifica che siano adottati tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati;

- impartisce le istruzioni e i comandi necessari per effettuare le copie di salvataggio;
- controlla che siano eseguiti salvataggi periodici dei dati con copie di backup;
- si assicura della qualità delle copie di backup dei dati e della loro conservazione in luogo adatto e sicuro;
- decide se i supporti di backup sono riutilizzabili e, in questo caso, con quale modalità e periodicità;
- protegge gli elaboratori dal rischi di intrusione (violazione del sistema da parte di "hackers") e dal rischio di virus informatici mediante idonei programmi;
- controlla periodicamente l'autoaggiornamento dei software antivirus e antispyware;
- effettua una scansione antivirus periodica sul server;
- effettua dal server una scansione antivirus sui client;
- gestisce la condivisione o meno delle risorse di rete;
- gestisce la condivisione delle stampanti in rete;
- imposta sugli elaboratori la scadenza trimestrale delle password di accreditamento all'accesso agli elaboratori stessi;
- controlla l'avvenuto cambio di password e controlla che le password siano alfanumeriche e di lunghezza minima di 8 caratteri;
- controlla che le password siano elaborate secondo le specifiche dell'All. B del D.lgs 196/2003.
- ha il compito di generare, sostituire ed invalidare, in relazione agli strumenti ed alle applicazioni informatiche utilizzate, le parole chiave ed i codici di accesso personali da assegnare agli incaricati del trattamento dati, nel rispetto delle massime misure di sicurezza.
- Gestisce il firewall del router (se presente) o dei singoli sistemi operativi;
- ha il compito di controllare periodicamente l'efficienza dei sistemi tecnici adottati e di redigere un apposito verbale, da consegnare al Titolare o al Responsabile, riportante i nominativi dei partecipanti al controllo, i riscontri e le verifiche effettuate, i parametri adottati e gli accorgimenti proposti per migliorare la sicurezza.

Via Zaccaria Pinto, 1
84078 *Vallo della Lucania* (SA)
Aut. 75

c.m. SAPS10000T
c.f. 84000540652

☎ 0974.4572
0974.719487
SAPS10000T@istruzione.it
(ministeriale)
liceoscientificov@tiscali.it

- Gestisce gli account di accesso agli elaboratori in accordo con quanto previsto dal Piano di Lavoro annuale dell'Istituto e in accordo con quanto dichiarato nel DPS.
- partecipe alla redazione del documento programmatico annuale, fornendo le proprie indicazioni e suggerimenti.
- Ha il compito di indicare al personale competente le modalità di distruzione e smaltimento dei supporti informatici di memorizzazione logica e di cancellazione dei dati per il loro reimpiego. Può anche provvedere direttamente.

L'Amministratore di Sistema svolgerà il proprio mandato presso IL LICEO SCIENTIFICO "DA VINCI", secondo le modalità e con gli strumenti tecnici messi a disposizione dal Titolare e dal Responsabile del Trattamento.

Nell'espletamento di tale attività, ai sensi del D. Lgs. 196/2003, dovrà attenersi alle misure di sicurezza definite nel "documento programmatico sulla sicurezza dei dati" iniziale e nelle sue successive revisioni.

Nello svolgimento di tale incarico dovrà comunque usare la massima riservatezza e discrezione in relazione ai dati di cui verrà a conoscenza curando attentamente al loro protezione ed attenersi alle istruzioni di carattere generale del Titolare.

Nel LICEO SCIENTIFICO "DA VINCI" l'Amministratore di Sistema è il D.S.G.A. che si avvale della collaborazione della SOCIETA' VELA NET in qualità di Società responsabile della manutenzione della rete della segreteria.

La presente nomina ha validità dal 01/12/2012

Data: 01/12/2012

**Firma del Titolare**

**Il Dirigente Scolastico**
***Prof. Antonio Iannuzzelli***

LICEO SCIENTIFICO STATALE
Leonardo da Vinci

Via Zaccaria Pinto, 1
84078 *Vallo della Lucania* (SA)
Aut. 75

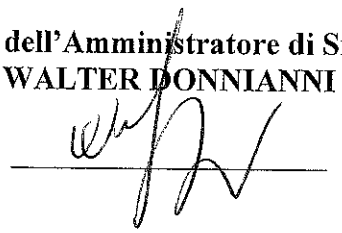
c.m. SAPS10000T
c.f. 84000540652

☎ 0974.4572
0974.719487
SAPS10000T@istruzione.it
(ministeriale)
liceoscientificov@tiscali.it

FESR
Unione Europea
FONDI STRUTTURALI EUROPEI
PON 2007-2013
MIUR
COMPETENZE PER LO SVILUPPO (FSE) - AMBIENTI PER L' APPRENDIMENTO (FESR)

Con la presente accetto la nomina ad Amministratore di sistema/custode delle credenziali di identificazione dei dati personali così come specificato nella lettera di nomina

**Firma dell'Amministratore di Sistema**
**WALTER DONNIANNI**



**Istruzioni per l'amministratore di sistema**

Le parole chiave devono essere utilizzate per accedere a differenti profili di autorizzazione, nell'ambito del sistema informativo aziendale.
Gli utilizzi più frequenti sono ad esempio: contabilità di utente, accesso ad Internet, accesso a sistemi di posta elettronica, accesso a screen saver, accesso a sistemi di casella elettronica vocale, e simili.

Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.
Il codice per l'identificazione (username), che l'amministratore del sistema provvede a fornire all'incaricato, quale componente della chiave per accedere all'elaboratore, e successivamente a gestire, deve essere univoco: esso non può essere assegnato ad altri incaricati, neppure in tempi diversi.

Le credenziali di autenticazione non utilizzate da almeno sei mesi devono essere disattivate salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.

La chiave per accedere agli strumenti deve essere disattivata, nei seguenti casi:

- immediatamente, nel caso in cui l'incaricato perda la qualità, che gli consentiva di accedere allo strumento (non solo se cessa di lavorare, presso il Titolare, ma anche , nel caso in cui che venga ad esempio trasferito da un ufficio all'altro, o da un'area ad un'altra con conseguente cambio delle mansioni e dei dati personali oggetto di trattamento, da cui dovesse conseguire l'attribuzione di una nuova chiave);

- in ogni caso, entro sei mesi di mancato utilizzo.
  Alla regola della disattivazione fa eccezione il caso delle *chiavi* che sono state *preventivamente autorizzate* per soli scopi di gestione tecnica, il cui utilizzo assume generalmente caratteristiche di occasionalità come ad esempio nel caso in cui l'amministratore di sistema ne necessiti una o due volte all'anno nel quadro della verifica globale sulla funzionalità complessiva del sistema.

Via Zaccaria Pinto, 1
84078 *Vallo della Lucania* (SA)
Aut. 75
c.m. SAPS10000T
c.f. 84000540652
☎ 0974.4572
0974.719487
SAPS10000T@istruzione.it
(ministeriale)
liceoscientificov@tiscali.it

L'accesso alle banche dati informatiche è possibile al personale dipendente e/o agli eventuali collaboratori coordinati e continuativi, autonomi che svolgano la loro attività per conto del Titolare, sempre che siano incaricati, tramite codice identificativo personale attribuito dall'Amministratore di Sistema e parola chiave sostituibile autonomamente dallo stesso dipendente.

Il codice identificativo viene disattivato dall'Amministratore di Sistema quando il soggetto perde la qualifica che ne permetteva l'uso o comunque secondo diversi criteri stabiliti dallo stesso. Ugualmente il codice viene disattivato in caso di mancato utilizzo dello stesso per almeno sei mesi.

L'Amministratore di Sistema:

- deve conferire solo all'apertura dell'utenza la parola chiave che poi viene autonomamente sostituita dal dipendente;
- l'Amministratore di Sistema stabilisce con la collaborazione del Responsabile dell'Ufficio Risorse Umane l'assegnazione e la revoca degli accessi assegnati agli Incaricati anche in caso di perdita della qualifica di incaricato o nel caso di trasferimento in altro ufficio.

L'amministratore di Sistema non deve permettere che soggetti non autorizzati abbiano accesso agli archivi automatizzati.

---

**ALLEGATO B.**

**DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA**
***(Artt. 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.
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.
3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.
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.

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.
6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.
7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
8. Le credenziali sono disattivate anche 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. 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.
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.

Sistema di autorizzazione

12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.
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. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Altre misure di sicurezza

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

Documento programmatico sulla sicurezza

19. Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:

19.1. l'elenco dei trattamenti di dati personali;
19.2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
19.3. l'analisi dei rischi che incombono sui dati;
19.4. le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonchè la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
19.5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;
19.6. la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonchè in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;
19.7. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;
19.8. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

Ulteriori misure in caso di trattamento di dati sensibili o giudiziari
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.
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.
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.
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.
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.

Misure di tutela e garanzia
25. Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.
26. Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.

Trattamenti senza l'ausilio di strumenti elettronici

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

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.

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.

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.