



**ISTITUTO TECNICO AERONAUTICO DI STATO  
"FRANCESCO DE PINEDO"**

00142 ROMA - Via F. Morandini, 30 - Tel. 06/5034141 – 06/5034143 - fax 06/5034160  
Distretto 19 - cod. mecc. RMTB010001

**Il Dirigente dell'istituzione Scolastica**

**Visto**

il decreto legislativo 30 giugno 2003, n.196 recante il Codice in materia di protezione di dati personali, e segnatamente gli artt. 34 ss., nonché l'allegato B del suddetto d.lgs., contenente il Disciplinare tecnico in materia di misure minime di sicurezza.

**Considerato**

che l'Istituzione Scolastica **Istituto Tecnico Aeronautico di Stato "Francesco De Pinedo"** con sede in Via Francesco Morandini, Roma in quanto dotata di un autonomo potere decisionale, ai sensi dell'art.28 del d.lgs. n. 196 del 2004, deve ritenersi titolare del trattamento di dati personali;

**Atteso**

che la suddetta Istituzione scolastica è tenuta a prevedere ed applicare le misure minime di sicurezza di cui agli artt. 31 e ss. del d.lgs. n.196 del 2003,

**Visto**

il "Regolamento sui dati sensibili e giudiziari del Ministero della pubblica Istruzione" contenuto nel Decreto Ministeriale n.305 del 7 Dicembre 2006

**adotta il presente**

**AGGIORNAMENTO AL**

**DOCUMENTO PROGRAMMATICO SULLA SICUREZZA**

**REDATTO AI SENSI E PER GLI EFFETTI DELL'ARTICOLO 34, COMMA 1, LETTERA G) DEL DLGS 196/2003, E DEL DISCIPLINARE TECNICO ALLEGATO AL MEDESIMO DECRETO SUB B)**

Il presente documento intende assolvere all'obbligo dell'adozione di un *documento programmatico sulla sicurezza*, imposto dal punto 19 del disciplinare tecnico allegato B al Dlgs. 30.6.2003 n. 196 pubblicato nel S.O. 123 alla G.U. 174 del 29.07.2003 in presenza di dati *sensibili o giudiziari*.

Il documento è redatto per definire e descrivere le politiche di sicurezza adottate dall' **Istituto Tecnico Aeronautico di Stato "Francesco De Pinedo" di Roma** ( d'ora in avanti sinteticamente nominato I.T.Aer. "De Pinedo") in materia di trattamento di dati personali ed i criteri organizzativi seguiti per la loro attuazione.

Il presente documento aggiorna il precedente di pari oggetto, accogliendo ed integrando quanto previsto dal Regolamento emesso dal M.P.I. Con detto decreto si elencano in modo organico, fonti e tipologie di dati sensibili e giudiziari e le relative operazioni per la gestione degli stessi nell'ambito del sistema dell'istruzione equindi all'interno di questo Istituto.

Il presente documento è redatto e firmato in calce dal titolare del trattamento I.T.Aer."De Pinedo" in persona del suo legale rappresentante prof. Antonio Misantone.

## Indice

Nel rispetto e con riferimento al disciplinare tecnico di cui sopra si forniscono idonee informazioni riguardanti:

1. Punto 19.1 del disciplinare:

***Elenco dei trattamenti di dati personali gestiti nell'Istituto***

- categorie di dati tipi e finalità dei dati trattati (crf decr. min. n.305 del 7/12/2006 )
- finalità del trattamento dei dati relativi ai fornitori
- strumenti utilizzati per il trattamento

2. Punto 19.2 del disciplinare:

***Distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati***

- organizzazione interna dell'Istituto
- organigramma sicurezza privacy e relative nomine
- istruzioni generali e impostazione metodologica

3. Punto 19.3 del disciplinare:

***Analisi dei rischi che incombono sui dati***

4. Punto 19.4 del disciplinare:

***Misure di sicurezza adottate e da adottare, per garantire l'integrità e la disponibilità dei dati, protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità***

- per calamità naturali
- per minacce intenzionali
- per minacce involontarie
- valutazione dei sistemi attuali e implementazioni previste

5. Punto 19.5 del disciplinare:

***criteri e le modalità di ripristino dei dati, in seguito a distruzione o danneggiamento***

6. Punto 19.6 del disciplinare:

***interventi formativi degli incaricati del trattamento***

7. Punto 19.7 del disciplinare:

***criteri da adottare, per garantire l'adozione delle misure minime di sicurezza, in caso di trattamenti di dati personali affidati all'esterno della struttura del titolare.***

8. Dichiarazioni d'impegno e firma

## **1. L'elenco dei trattamenti dei dati personali gestiti dallo Istituto Tecnico Aeronautico " Francesco De Pinedo "**

### 1.1 Tipi e categorie di dati trattati dal Titolare si possono suddividere come segue:

I tipi di dati trattati da questa amministrazione sono quelli elencati nell'allegato regolamento del ministero della pubblica istruzione con decreto ministeriale n.305 del 7 dicembre 2006, in particolare si vedano le schede dalla n.1 alla n.5 e la n.7 ( la scheda n.6 non è applicabile ).

In particolare si accoglie e si riassumono i dati trattati per categorie secondo il seguente schema:

<b>Scheda n.</b>	<b>Contesto del trattamento</b>
1	Selezione e reclutamento a tempo indeterminato e determinato e gestione del rapporto di lavoro
2	Gestione del contenzioso e procedimenti disciplinari
3	Organismi collegiali e commissioni istituzionali
4	Attività propedeutiche all'avvio dell'anno scolastico
5	Attività Educativa didattica e formativa di valutazione
6	NON APPLICABILE ( Scuole non statali )
7	Rapporti scuola-famiglia, gestione del contenzioso

### 1.2 I dati relativi ai fornitori sono trattati per le seguenti finalità:

- attività e acquisti connessi alle iniziative dell' I.T.Aer."F. De Pinedo" per la fornitura dei Servizi agli utenti direttamente o mediante la conclusione di contratti con terzi soggetti e/o società, in qualità di autonomi titolari o di responsabili del trattamento dei Dati Personali, nonché per l'acquisizione di informative precontrattuali ;
- gestione dei contenziosi eventualmente verificatisi o in essere presso le autorità giudiziarie

### 1.3 Strumenti utilizzati per il trattamento.

#### **Schedari ed altri supporti cartacei**

I supporti cartacei, ivi inclusi quelli contenenti immagini, vengono ordinatamente raccolti in schedari diversi per ogni reparto, ovvero nella pratica cui si riferiscono, per essere archiviati una volta terminato il ciclo lavorativo, come segue:

- archivi di pratiche di natura comune e sensibile relative a utenti e fornitori
- archivi di pratiche di natura comune e sensibile relative al personale
- archivi di pratiche di natura sensibile relative a soggetti diversi dal personale

### **Elaboratori in rete privata**

Per elaboratori in rete privata si intendono quelli accessibili, da altri elaboratori o più in generale da altri strumenti elettronici, solo attraverso reti proprietarie, sulle quali possono viaggiare unicamente i dati del titolare del sistema.

- Si dispone di una rete che serve gli uffici amministrativi, costituita da un minimo di 13 Personal Computer dipendenti da un Server. La rete é realizzata mediante collegamenti interni via cavo.
- La rete ha due accessi verso l'esterno sulla rete internet a mezzo di linee adsl dedicate e protette da due firewall hardware diversamente configurati a seconda delle esigenze
- La rete è inoltre collegata alla intranet ministeriale tramite il sistema SIMPI, ma con accesso dedicato su un solo PC della rete

### **Altri strumenti.**

Vengono inoltre utilizzati dei personal computer con programmi dedicati alla presidenza e alla segreteria didattica per la gestione delle presenze, nonché per la gestione di scrutini e pagelle e comunicazioni sms con le famiglie.

La gestione di detti programmi è comunque tale da dover considerare l'utilizzo degli strumenti informatici alla stregua di "macchine da scrivere". I dati trattati non vengono memorizzati in modo permanente ma gestiti in modalità cartacea per tutte le modalità di archiviazione.

## 2. Distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati

### 2.1 Organizzazione interna dell'Istituto

Per il trattamento di dati personali dei soggetti su menzionati è suddivisa in cinque macro aree operative da ora denominate **unità operative**, in funzione dei soggetti dei quali vanno a trattare i dati personali.

Unità operative	Soggetti interessati al trattamento dei dati
<b>Didattica</b>	Utenza ( composta da alunni e famiglie )
<b>Amministrativa</b>	Personale docente e utenza
<b>Ata</b>	Personale ATA
<b>Attività di volo</b>	Utenza e fornitori di servizi
<b>Magazzino</b>	Fornitori

Le varie unità operative sono organizzate come descritto negli schemi che seguono, e trattano dati personali, descritti secondo quanto riportato nel regolamento dati sensibili del M.P.I. e nelle schede sottoindicate

Tabella 1					
Unità operativa: <b>DIDATTICA</b>			ubicazione: <b>piano terra</b>		
schede	Soggetti interessati	Azioni	Banca dati elettronica	Archivio cartaceo	Incaricati
4, 5, 7	Studenti e famiglie	Fascicoli personali	Si	Si	Rocchino, Felici Sorace
4, 5	Studenti e famiglie	Esonero religione	Si	Si	
3	Famiglie	Organi collegiali	Si	Si	

Tabella 2					
Unità operativa: <b>AMMINISTRATIVA</b>			ubicazione: <b>I piano</b>		
schede	Soggetti interessati	Azioni	Banca dati elettronica	Archivio cartaceo	Incaricati
1, 2, 3	Docenti	Fascicoli personali, contratti , graduatorie, TFR	SI	SI	Mulas/Piro
1, 2, 3	Docenti Docenti e alunni	Comunicazione scioperi malattie e infortuni	No	SI	Mulas
1, 2, 3	Docenti	Contratti docenti T.I. – T.D.	No	SI	Mulas/Piro
3, 7	Famiglie	Comunicazioni	SI	SI	tutti
1	Docenti, ditte, alunni enti	Contabilità retribuzioni	SI	SI	Scippa Gatti
1	Docenti, ditte, alunni enti	Ritenute sindacali	SI	SI	
7	Docenti, ditte, alunni enti	Contenziosi	SI	SI	
1, 2, 3, 4, 5, 7	tutti	Protocollo	NO	SI	Roganti
1	tutti	Contratti	NO	SI	

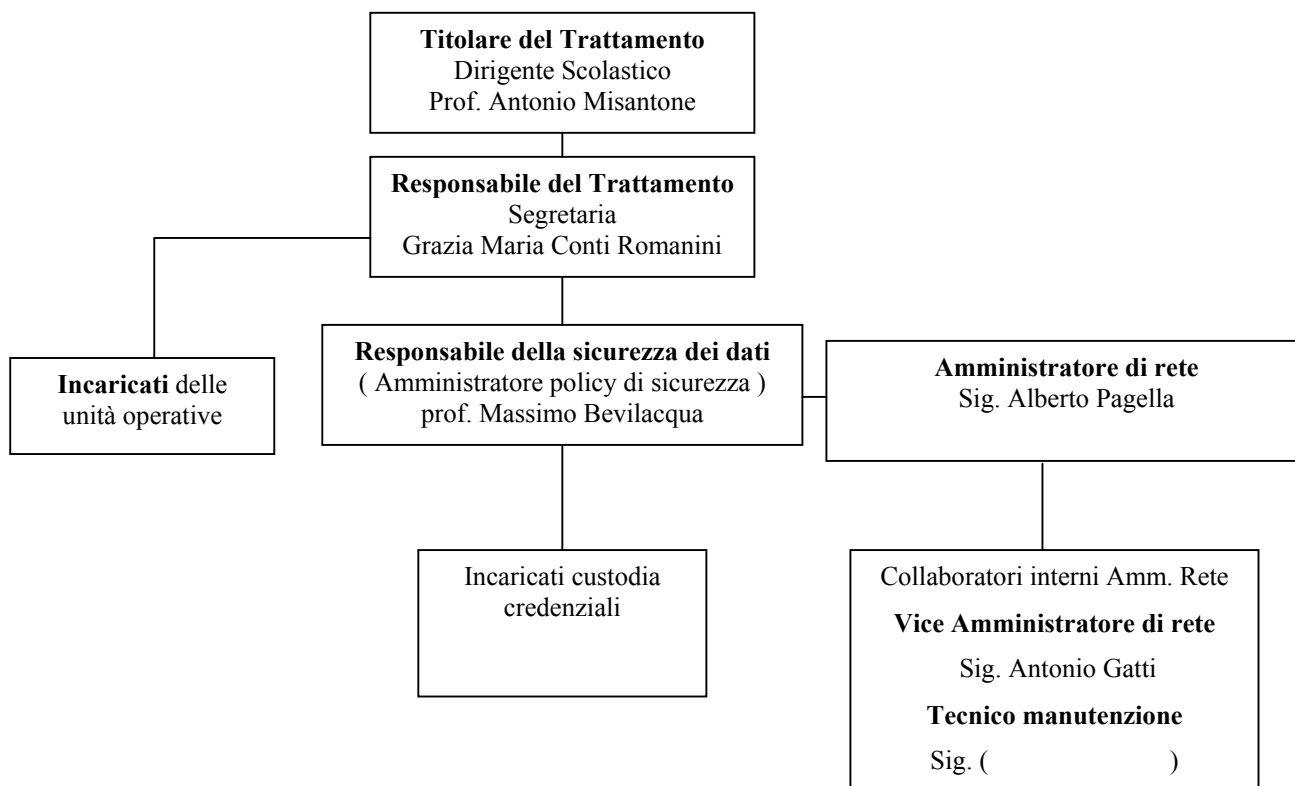
<b>Tabella 3</b>					
<b>Unità operativa: ATTIVITA' DI VOLO</b>				<b>ubicazione: I piano</b>	
<b>schede</b>	<b>Soggetti interessati</b>	<b>Azioni</b>	<b>Banca dati elettronica</b>	<b>Archivio cartaceo</b>	<b>Incaricati</b>
5	STUDENTI	ATT. DI VOLO	SI	SI	Basta
5	STUDENTI	ATT. DI VOLO ( Istituto di Medicina Legale )	SI	SI	
5, 7	SCUOLE DI VOLO	AGGIUDICAZIONE BANDO DI GARA (CONTENZIOSI)	SI	SI	

<b>Tabella 4</b>					
<b>Unità operativa: ATA</b>			<b>ubicazione: I piano</b>		
<b>schede</b>	<b>Soggetti interessati</b>	<b>Azioni</b>	<b>Banca dati elettronica</b>	<b>Archivio cartaceo</b>	<b>Incaricati</b>
1, 2, 3	PERSONALE ATA	GESTIONE FASCICOLI PERSONALI	SI	SI	COFONE
1, 2, 3	PERSONALE ATA	CASELLARIO	NO	SI	

<b>Tabella 5</b>					
<b>Unità operativa: MAGAZZINO</b>			<b>ubicazione: I piano</b>		
<b>schede</b>	<b>Soggetti interessati</b>	<b>Azioni</b>	<b>Banca dati elettronica</b>	<b>Archivio cartaceo</b>	<b>Incaricati</b>
1	Fornitori	Ordini di acquisto	SI	SI	De Giudice Piro Basta

## 2.2 Organigramma Sicurezza Privacy

Suddivise le attività secondo le unità operative sopra descritte, il Titolare ha quindi strutturato il seguente organigramma della sicurezza privacy :



### Sono stati nominati :

- **un responsabile unico interno per il trattamento dei dati,** nella persona della sig.ra Grazia Maria Conti Romanini ;
- **un responsabile interno per la sicurezza dei dati personali,** nella persona del prof. Massimo Bevilacqua
- **un amministratore di rete ( esterno )** nella persona del sig. Alberto Pagella
- **un vice amministratore di rete ( interno ),** nella persona del Sig. Antono Gatti
- **un tecnico interno addetto alla manutenzione dei sistemi,** nella persona del sig. ( si vedano allegati e mansionario )

### 2.3 Istruzioni generali e impostazione metodologica

Il trattamento dei dati personali viene effettuato solo da **soggetti che hanno ricevuto un formale incarico**, mediante designazione per iscritto di ogni singolo incaricato, con la quale si individua puntualmente l'ambito del trattamento consentito.

Oltre alle istruzioni generali, su come devono essere trattati i dati personali, agli incaricati vengono fornite esplicite istruzioni in merito ai seguenti punti, aventi specifica attinenza con la sicurezza:

- 1) procedure da seguire per la classificazione dei dati, al fine di distinguere quelli sensibili e giudiziari, per garantire la sicurezza dei quali occorrono maggiori cautele, rispetto a quanto è previsto per i dati di natura comune
- 2) modalità di reperimento dei documenti, contenenti dati personali, e modalità da osservare per la custodia degli stessi e la loro archiviazione, al termine dello svolgimento del lavoro per il quale è stato necessario utilizzare i documenti
- 3) modalità per elaborare e custodire le password, necessarie per accedere agli elaboratori elettronici ed ai dati in essi contenuti, nonché per fornirne una copia al preposto alla custodia delle parole chiave
- 4) prescrizione di non lasciare incustoditi e accessibili gli strumenti elettronici, mentre è in corso una sessione di lavoro mediante:
  - a. screen-saver con password
  - b. procedure e modalità di utilizzo degli strumenti e dei programmi atti a proteggere i sistemi informativi
  - c. procedure per il salvataggio dei dati
  - d. modalità di custodia ed utilizzo dei supporti rimovibili, contenenti dati personali
  - e. dovere di aggiornarsi, utilizzando anche il materiale e gli strumenti forniti dal Titolare, sulle misure di sicurezza.

Ai soggetti incaricati della gestione e manutenzione del sistema informatico, siano essi interni o esterni all'organizzazione del Titolare, viene prescritto di non effettuare alcun trattamento, sui dati personali contenuti negli strumenti elettronici, fatta unicamente eccezione per i trattamenti di carattere temporaneo strettamente necessari per effettuare la gestione o manutenzione del sistema.

Le lettere ed i contratti di nomina dei responsabili, le lettere di incarico o di designazione degli incaricati vengono raccolte in modo ordinato, in base ai reparti cui i soggetti appartengono: in tale modo il Titolare dispone di un quadro chiaro di chi fa cosa (*mansionario privacy*), nell'ambito del trattamento dei dati personali.

Periodicamente, con cadenza almeno annuale, si procede ad aggiornare la definizione dei dati cui gli incaricati sono autorizzati ad accedere, e dei trattamenti che sono autorizzati a porre in essere, al fine di verificare la sussistenza delle condizioni che giustificano tali autorizzazioni.

La stessa operazione viene compiuta per le autorizzazioni rilasciate ai soggetti incaricati della gestione o manutenzione degli strumenti elettronici.

Sono previsti **interventi formativi degli incaricati del trattamento**, finalizzati a renderli edotti dei seguenti aspetti:

- profili della disciplina sulla protezione dei dati personali, che appaiono più rilevanti per l'attività svolta dagli incaricati, e delle conseguenti responsabilità che ne derivano
- rischi che incombono sui dati
- misure disponibili per prevenire eventi dannosi
- modalità per aggiornarsi sulle misure di sicurezza, adottate dal titolare.

Tali interventi formativi sono programmati in modo tale, da avere luogo al verificarsi di una delle seguenti circostanze:

- già al momento dell'ingresso in servizio
- in occasione di cambiamenti di mansioni, che implicino modifiche rilevanti rispetto al trattamento di dati personali
- in occasione della introduzione di nuovi significativi strumenti, che implicino modifiche rilevanti nel trattamento di dati personali.

Gli interventi formativi possono avvenire sia all'interno, a cura del responsabile per la sicurezza o di altri soggetti esperti nella materia, che all'esterno, presso soggetti specializzati.

### **3. Analisi dei rischi che incombono sui dati**

I rischi che incombono sui dati ( sia su cartaceo che supporto informatico ) sono stati valutati suddividendoli come segue :

#### **a) Calamità naturali:**

1. Perdita di dati conseguente ad allagamento
2. Perdita di dati conseguente ad incendio

#### **b) Minacce intenzionali**

1. Accessi *non consentiti*:
  - a) Accesso, furto, manomissione di dati su supporti cartacei
  - b) Accesso, furto, manomissione di dati su supporti informatici
2. Accessi *non autorizzati* ( trattamento di dati eseguito da personale non incaricato )
3. Perdita di dati dovuta a virus o ad intrusione informatica

#### **c) Minacce involontarie**

1. Black out elettrico
2. Malfunzionamenti nel software
3. Malfunzionamenti hardware
4. Errori degli incaricati

#### 4. Misure atte a garantire l'integrità e la disponibilità dei dati

Con riferimento alla analisi di cui al precedente punto 3 si predispongono le seguenti misure minime di protezione:

##### 4.1 Calamità naturali:

###### 4.1.1 Perdita di dati conseguente ad allagamento:

Per ciò che concerne il rischio di perdita di dati da allagamento, considerata la posizione del fabbricato si esclude che, salvo eventi imprevedibili e del tutto eccezionali, detto rischio possa verificarsi.

Ad ogni modo le attrezzature informatiche sono state tutte rialzate da terra.

###### 4.1.2 Perdita di dati conseguente ad incendio:

Per ciò che concerne la perdita di dati conseguente ad incendio si precisa che sono state attuate tutte le misure previste dall'attuale legislazione in materia di prevenzione incendi, inclusa la verifica periodica di caldaie, impianto elettrico, impianto di riciclo d'aria e condizionamento; si precisa inoltre che la posizione di estintori risulta dalla planimetria affissa in duplice copia nei locali dell'Istituto richiamando inoltre le norme di comportamento da seguire in caso di incendio, anch'esse affisse nei locali.

##### 4.2 Minacce intenzionali

###### 4.2.1. Accessi non consentiti:

###### a) Accesso, furto, manomissione di dati **su supporti cartacei**

Si evidenzia che:

- Gli ingressi dell'Istituto sono protetti da cancellate, nonché da un sistema di allarme automatico collegato con una centrale di controllo operativa di un servizio di polizia privato, che viene attivato alla chiusura dell'Istituto
- I locali nei quali si svolge il trattamento sono protetti da: cancelli metallici con serratura, e sistema elettrico apri porta e vigilanza da parte di personale interno.

Gli incaricati devono custodire in modo appropriato gli atti, i documenti ed i supporti contenenti dati personali, loro affidati per lo svolgimento delle mansioni lavorative.

Cautele particolari sono previste per gli atti, documenti e supporti contenenti dati sensibili e giudiziari: agli incaricati viene in questi casi prescritto di provvedere al controllo ed alla custodia in modo tale, che ai dati non possano accedere persone prive di autorizzazione. A tale fine, gli incaricati sono stati dotati di:

- Armadi con serrature
- Cassettiere e raccoglitori con serrature
- Scrivanie personali a cassetti con chiave

nei quali devono riporre i documenti, contenenti dati sensibili o giudiziari, prima di assentarsi dal posto di lavoro, anche temporaneamente. In tali dispositivi i documenti possono essere riposti anche al termine della giornata di lavoro, qualora l'incaricato debba continuare ad utilizzarli, nei giorni successivi.

Al termine del trattamento, l'incaricato dovrà invece restituire all'archivio gli atti, i documenti ed i supporti, non più necessari per lo svolgimento delle proprie mansioni lavorative.

Per quanto concerne l'archiviazione, il Titolare ha adibito apposite aree, nelle quali conservare ordinatamente documenti, atti e supporti contenenti dati personali, in modo distinto per le diverse funzioni aziendali.

Particolari cautele sono previste per l'archiviazione di documenti, atti e supporti contenenti dati sensibili o giudiziari: essa deve avvenire in luoghi, armadi, casseforti o dispositivi equipollenti, che possono essere chiusi.

Gli archivi contenenti dati sensibili o giudiziari sono controllati, mediante l'adozione dei seguenti accorgimenti:

- ad alcune persone, aventi la scrivania prospiciente, viene dato l'incarico di vigilare gli archivi, dettando precise istruzioni in merito al fatto che una persona deve essere sempre presente, durante l'orario di apertura dell'archivio, per controllare chi vi accede.
- Si procede inoltre ad identificare e registrare le persone che accedono agli archivi, contenenti dati sensibili o giudiziari,

Dopo l'orario di chiusura, non è possibile accedere agli archivi a persone diverse dal titolare, dal responsabile o, eccezionalmente, a un suo delegato.

Gli impianti ed i sistemi di cui è dotata l'organizzazione appaiono soddisfacenti, al fine di garantire le opportune misure di sicurezza, al trattamento di dati personali da essa svolti. Per gli anni successivi sono quindi previsti semplicemente interventi di manutenzione.

b) Accesso, furto, manomissione di dati **su supporti informatici**.

Per gli elaboratori elettronici, sono poste in essere le stesse misure fisiche di protezione elencate per gli archivi cartacei.

Le protezioni minime non si sono rivelate sufficienti ad impedire una serie di furti del materiale informatico. Le protezioni ( fisiche e di sorveglianza ) non sono risultate adeguate per motivi riconducibili a cattiva gestione da parte della Provincia dei sistemi di allarme ( alla Provincia spetta stabilire contratti e modalità dei servizi di allarme e sorveglianza, nonché l'installazione di adeguate protezioni fisiche anti-intrusione ).

L'istituto, da parte sua, a seguito di ripetuti furti dei sistemi informatici ha verificato l'efficacia dei sistemi di backup adottati, ristabilendo il funzionamento delle banche dati nell'arco di 48 ore dalla installazione di nuovi P.C.

Inoltre, si ritiene di incrementare ulteriormente la sicurezza, spostando in zona più protetta il server e dotando gli ambienti della segreteria amministrativa di telecamere a circuito chiuso ad infrarossi, con sistema di registrazione delle immagini.

Detto sistema video sarà programmato per entrare in funzione in orario diverso da quello di servizio ed in particolare nei giorni e nelle ore di chiusura della scuola ( onde garantire gli operatori della necessaria privacy ).

Si aggiunge un sistema di bloccaggio dei PC alle scrivanie, onde rendere anti economico il furto delle macchine a causa del danneggiamento delle stesse.

#### 4.2.2. Accessi non autorizzati

Per quanto concerne le tipologie di dati ai quali gli incaricati possono accedere, ed i trattamenti che possono effettuare, si osserva che, all'interno dei software gestionali utilizzati, sono previsti profili di autorizzazione distinti, per le diverse persone, in relazione alla organizzazione interna dell'Istituto; tenuto conto che uno o più incaricati possano accedere ad alcune tipologie di dati personali oggetto di trattamento e non ad altri.

La possibilità di accessi non autorizzati dipende quindi dalla diligenza con cui i vari operatori si attengono alle seguenti disposizioni, da ora complessivamente denominate **"policy di sicurezza informatica"** :

- si associa un codice per l'identificazione dell'incaricato (username), attribuito da chi amministra il sistema, ad una parola chiave riservata (password), conosciuta solamente dall'incaricato, che provvederà ad elaborarla, mantenerla riservata e modificarla periodicamente

Per l'attribuzione e la gestione delle credenziali per l'autenticazione si utilizzano i seguenti criteri:

- le credenziali vengono assegnate o associate ad ogni incaricato individualmente, per cui non è ammesso che due o più incaricati possano accedere agli strumenti elettronici utilizzando la medesima credenziale.
- Il codice per l'identificazione (username), attribuito all'incaricato da chi amministra il sistema, è univoco: esso non può essere assegnato ad altri incaricati, neppure in tempi diversi.
- Viene segnalato agli incaricati che la lunghezza della password da utilizzare non deve essere inferiore ad otto caratteri, salvo limitazioni tecniche nei software in uso.
- Agli incaricati è prescritto di utilizzare alcuni accorgimenti, nell'elaborazione delle password:
  - o non devono contenere riferimenti agevolmente riconducibili all'interessato (non solo nomi, cognomi, soprannomi, ma neppure date di nascita proprie, dei figli o degli amici), né consistere in nomi noti, anche di fantasia (pippo, pluto, paperino)
  - o buona norma è che, dei caratteri che costituiscono la password, da un quarto alla metà siano di natura numerica.
  - o La password non deve essere comunicata a nessuno (non solo a soggetti esterni, ma neppure a persone appartenenti all'organizzazione, siano esse colleghi, responsabili del trattamento, amministratore del sistema o titolare).

**Nei casi di prolungata assenza o impedimento dell'incaricato**, che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, potrebbe però rendersi necessario disporre della password dell'incaricato, per accedere agli strumenti ed ai dati. A tale fine, agli incaricati sono state fornite istruzioni scritte, affinché essi:

- scrivano la parola chiave su un foglio di carta, da inserire in una busta che deve essere chiusa e sigillata

- consegnino la busta a chi custodisce le copie delle parole chiave, il cui nominativo viene loro indicato al momento dell'attribuzione della password.

Solo al verificarsi delle condizioni, sopra esposte, che rendono necessario accedere allo strumento elettronico, utilizzando la copia della parola chiave, il titolare o un responsabile potranno richiedere la busta che la contiene, a chi la custodisce. Dell'accesso effettuato si dovrà provvedere ad informare, tempestivamente, l'incaricato cui appartiene la parola chiave.

Viene segnalato ad ogni incaricato la necessità di cambiare la password almeno ogni 6 mesi.

**Nell'ipotesi di trattamento di dati sensibili** viene segnalato ad ogni incaricato la necessità di cambiare la password almeno ogni 3 mesi.

Al verificarsi dei seguenti casi, è prevista la disattivazione delle credenziali di autenticazione:

- immediatamente, nel caso in cui l'incaricato perda la qualità, che gli consentiva di accedere allo strumento
- in ogni caso, entro sei mesi di mancato utilizzo.

Il sistema di identificazione ed autenticazione è operativo anche sui computer portatili e sui palmari che possono gestire e contenere dati personali .

**Per quanto concerne i supporti rimovibili** (es. floppy disk, chiavette hard disk, cd riscrivibili ZIP,...), contenenti dati personali, la norma impone particolari cautele solo nell'ipotesi in cui essi contengano dati sensibili o giudiziari.

L'istituto ha ritenuto di estendere tali precetti ai supporti contenenti dati personali di qualsiasi natura, anche comune, prescrivendo agli incaricati del trattamento quanto segue:

    i supporti devono essere custoditi ed utilizzati in modo tale, da impedire accessi non autorizzati (furti inclusi) e trattamenti non consentiti: in particolare, essi devono essere conservati in cassette chiuse a chiave, durante il loro utilizzo, e successivamente formattati, quando è cessato lo scopo per cui i dati sono stati memorizzati su di essi, una volta cessate le ragioni per la conservazione dei dati, si devono in ogni caso porre in essere gli opportuni accorgimenti, finalizzati a rendere inintelligibili e non ricostruibili tecnicamente i dati contenuti nei supporti.

Tali dati devono quindi essere cancellati, se possibile, e si deve arrivare addirittura a distruggere il supporto, se necessario per i fini in esame.

#### 4.2.3. Perdita di dati dovuta a virus od intrusione informatica

##### *a) a causa di Virus informatici*

Per ciò che concerne la perdita di dati o di danneggiamento degli stessi dovuta a virus, si precisa che la rete degli uffici è protetta come segue :

##### Server:

Sistema antivirus NOD32 + sistema antispam SpySweeper Winrooute.

##### Client:

Sistema antivirus AVG o equivalente

Gli antivirus descritti controllano in automatico ogni file scaricato dalla rete o dalla posta elettronica o letto da supporti esterni quali floppy disk e cd rom.

Il personale viene adeguatamente informato sui comportamenti corretti da tenere per evitare di introdurre virus informatici nella rete scolastica.

L'aggiornamento alle nuove definizioni dei virus avviene, per i personal computers, manualmente ogni 30 giorni collegandosi al sito dell'azienda produttrice dell'antivirus e scaricando l'aggiornamento.

##### *b) Intrusione informatica*

##### Server:

Il server è protetto da una DMZ grazie all'utilizzo di un firewall di tipo hardware

##### Client:

Due firewall di tipo hardware sono diversamente configurati in modo da proteggere opportunamente i client, a seconda dell'utilizzo tipico.

#### 4.3 Minacce involontarie

##### ***Black out elettrico***

E' stato installato un semplice sistema con batteria tampone per salvaguardare il server da sbalzi di tensione o improvvise mancanze di corrente.

Verrà sostituito con un sistema che garantisca almeno due ore di funzionamento autonomo su server e firewall.

### ***Malfunzionamenti nel software***

Viene eseguito un backup settimanale dei dati elaborati con il software AXIOS eseguito dal vice amministratore di rete

### ***Malfunzionamenti hardware***

I malfunzionamenti di questo tipo sono stati considerati critici solo sul server. Per questo l'amministratore di rete esegue una periodica immagine del disco da remoto, onde ripristinare immediatamente il sistema in caso di danno grave dell' HD.

### ***Errori degli incaricati***

Per quanto riguarda un eventuale danneggiamento software degli archivi sarà necessario ricaricare l'ultimo backup e riportarsi alla situazione della data del backup, perdendo ovviamente, le ultime transazioni.

#### **4.4 Valutazione dei sistemi attuali e implementazioni previste**

Si ritiene il sistema attuale sia adeguato per quanto riguarda il rischio di malfunzionamenti hardware.

Modalità e tempistiche dei backup e delle simulazioni di ripristino vengono specificate nel mansionario privacy

Si sono realizzati e o pianificati i seguenti interventi di adeguamento:

- La protezione da black out richiede l'acquisto di un gruppo APC da almeno 1500VA in onda sinusoidale.
- si dispone di due linee internet con sistema firewall fisico differenziato in funzione delle attività da svolgere negli uffici ed in particolare, con criteri di protezione differenti a seconda del rischio di esposizione verso l'esterno, già verificato su alcune macchine

## **5. Criteri e modalità di ripristino dei dati, in seguito a distruzione o danneggiamento**

I dati gestiti dalla rete oggetto del presente dps sono normalmente gestiti con una molteplicità di software a seconda delle funzioni.

### Per quanto gestito da software AXIOS:

il software è installato separatamente su ogni macchina oltre che sul server, il relativo database è invece installato solamente sul server.

Le procedure di backup dei dati sono accessibili da ogni macchina ma creano set di backup locali che possono creare fraintendimenti ed errori in caso di ripristino.

I profili di accesso degli utenti vengono stabiliti con l'uso di un software specifico installato solo sul pc del Responsabile del trattamento.

Visto il funzionamento tipico e gli inconvenienti descritti dagli incaricati si ritiene necessario verificare quanto segue:

- 1) Gli aggiornamenti eseguiti dal personale axios devono essere sempre realizzati su TUTTI i pc della rete, di questa funzione sarà responsabile il vice amministratore.
- 2) La configurazione degli accessi deve essere ripetuta/verificata ad ogni aggiornamento a cura del responsabile della sicurezza o a cura del responsabile del trattamento
- 3) Alla ditta axios è stato necessariamente assegnato un accesso di tipo power user sul server;

### Per quanto attiene a dati gestiti con altri software ( entratel ecc...),

questi vengono salvati sulle postazioni locali e poi utilizzati in modo cartaceo tradizionale.

## **Procedure di copia, verifica e ripristino per ogni singola unità contenente dati**

### Unità contenenti dati

I dati di carattere esclusivamente informatico da proteggere sono distribuiti come segue

1. dati personali gestiti dal software axios : contenuti nel relativo database sull'unità server
2. dati personali gestiti a mezzo entratel e altri software di comunicazione con enti ed istituzioni :  
su singole postazioni PC

Si ritiene di dover assicurare una particolare protezione solo alla prima categoria di dati, di conseguenza il Vice amministratore di rete provvede ad eseguire una copia di backup settimanale a mezzo software axios su un PC in locale e su VDV RAM. E l'amministratore esegue la già menzionata immagine del disco da remoto su HD remoto.

Si valuta la possibilità di creare una immagine disco su DVD per il PC che gestisce programmi entratel e affini.

## **Salvataggio ulteriore dei dati**

Oltre al backup settimanale, il database axios viene salvato a mezzo copia fisica locale o su DVD RAM almeno due volte al mese

### **Ripristino dei dati**

Il tempo necessario per recuperare i dati dalle copie di sicurezza, a fronte di una generica emergenza, viene stimato in poche ore dal verificarsi del possibile accadimento negativo, comunque ampiamente sotto il limite dei sette giorni previsti dal punto 23 dell'allegato B del D.Lgs. 196/2003 in ipotesi di trattamento di dati sensibili.

Non si ritiene di testare il sistema di ripristino a mezzo simulazioni in quanto a seguito di furto delle macchine è stata verificata l'efficacia del sistema che ha consentito ( dopo la re-istallazione delle macchine ) di recuperare gli archivi entro i tempi previsti dalla normativa

## **6. interventi formativi degli incaricati del trattamento**

L'Azienda riconosce l'importanza della formazione dei suoi componenti riguardo le tematiche della sicurezza, come elemento significativo di riduzione dei rischi al proprio sistema informativo e s'impegna a promuovere momenti formativi, in particolare al momento dell'ingresso in servizio o al momento di cambiamenti di mansioni di tali soggetti o all'introduzione di nuovi strumenti elettronici che hanno impatto sul trattamento dei dati personali.

Tutti i componenti dell'Azienda devono comunque partecipare una volta all'anno ad un corso di approfondimento e mantenimento delle conoscenze finalizzati a renderli edotti dei seguenti aspetti:

- profili della disciplina sulla protezione dei dati personali, che appaiono più rilevanti per l'attività svolta dagli incaricati, e delle conseguenti responsabilità che ne derivano
- utilizzo dei sistemi antivirus
- rischi che incombono sui dati
- misure disponibili per prevenire eventi dannosi
- modalità per aggiornarsi sulle misure di sicurezza.

Gli interventi formativi possono avvenire:

- All'interno, a cura del titolare, di persone da questo incaricate o di altri soggetti esperti nella materia
- All'esterno a cura di enti, istituzioni e/o associazioni qualificate

## 7. Affidamento di dati personali all'esterno

Nei casi in cui i trattamenti di dati personali vengano affidati, in conformità a quanto previsto dal Dlgs 196/2003, all'esterno della struttura del Titolare, si adottano i seguenti criteri, atti a garantire che il soggetto destinatario adotti misure di sicurezza conformi a quelle minime, previste dagli articoli da 33 a 35 Dlgs 196/2003 e dal disciplinare tecnico, allegato sub b) al codice.

Per la generalità dei casi, in cui il trattamento di dati personali, **di qualsiasi natura**, venga affidato all'esterno della struttura del titolare, sono impartite istruzioni per iscritto al terzo destinatario, di rispettare quanto prescritto per il trattamento dei dati personali:

- dal Dlgs 196/2003, se il terzo destinatario è italiano
- dalla direttiva 95/46/CE, se il terzo destinatario non è italiano.

Qualora il trasferimento avvenga verso soggetti residenti in Paesi extra-Ue, che non sono considerati sicuri per il trattamento di dati personali, si stipulano con il destinatario clausole contrattuali conformi, per quanto concerne le misure di sicurezza, a quanto previsto dalla decisione 2002/16/CE: eccezione può essere fatta nei casi, previsti dall'articolo 43 Dlgs 196/2003, in cui il trasferimento può avvenire senza che vengano stipulate tali clausole.

Nei casi in cui il trattamento affidato all'esterno abbia per oggetto dati **sensibili o giudiziari**, si procede alla stipula di clausole contrattuali, con il destinatario, che disciplinano gli aspetti legati alla gestione dei dati personali: se il destinatario è residente in Paesi extra-Ue, che non sono considerati sicuri per il trattamento di dati personali, tali clausole sono conformi, per quanto concerne le misure di sicurezza, a quanto previsto dalla decisione 2002/16/CE.

Nell'ipotesi in cui il trattamento, di dati sensibili o giudiziari, avvenga con strumenti elettronici, si esige inoltre che il destinatario italiano rilasci la dichiarazione di avere redatto il documento programmatico sulla sicurezza, nel quale abbia attestato di avere adottato le misure minime previste dal disciplinare tecnico.

Nei casi in cui ciò si renda opportuno, per ragioni operative legate anche alla tutela dei dati personali, il destinatario esterno viene nominato dal Titolare come responsabile del trattamento dei dati, mediante apposita lettera scritta.

## **8. Dichiarazioni d'impegno e firma.**

Il presente documento, redatto il, viene firmato in calce da:

Antonio Misantone, in qualità di rappresentante legale dell'Istituto;

L'originale del presente documento viene custodito presso la sede dell'Azienda, per essere esibito in caso di controlli.

Viene attribuita data certa a mezzo deposito al Protocollo di Istituto

Una sua copia verrà consegnata:

- a ciascun responsabile interno del trattamento dei dati personali

ROMA, 28/3/2007

Firma del rappresentante  
legale dell'Istituto

Dati di consegna al protocollo