

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Titolare del ISTITUTO DI ISTRUZIONE SUPERIORE “PRIMO LEVI”
Trattamento: DIRIGENTE SCOLASTICO PROF. LAMBERTO PILLONETTO

Art. 34 D.Lgs
n. 196/2003

Prot. n° 2448/C14

IN OTTEMPERANZA A QUANTO PREVISTO DAL TESTO UNICO SULLA PRIVACY

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA [D.Lgs. 196/03]

**Istituto di Istruzione Superiore
“Primo Levi” di MONTEBELLUNA**

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Titolare del **ISTITUTO DI ISTRUZIONE SUPERIORE "PRIMO LEVI"** **Art. 34 D.Lgs**
Trattamento: **DIRIGENTE SCOLASTICO PROF. LAMBERTO PILLONETTO** **n. 196/2003**

INDICE

1	SCOPO E AMBITO DI APPLICAZIONE DEL DPS	3
2	OBBLIGO DI LEGGE: REDAZIONE DEL DOCUMENTO.....	3
3	REVISIONI	4
4	DEFINIZIONI	5
5	TIPI DI DATI E TIPI DI TRATTAMENTI.....	7
6	FIGURE PREVISTE PER LA SICUREZZA DEI DATI PERSONALI.....	8
6.1	TITOLARE DEL TRATTAMENTO DEI DATI PERSONALI	8
6.2	RESPONSABILE DELLA SICUREZZA E DEL TRATTAMENTO DEI DATI PERSONALI ..	8
6.3	RESPONSABILE DELLA GESTIONE E MANUTENZ. DEGLI STRUMENTI ELETTRONICI .	9
6.4	INCARICATO DELLA GESTIONE DELLE COPIE DELLE CREDENZIALI.....	10
6.5	INCARICATO DELLE COPIE DI SICUREZZA DELLE BANCHE DATI	11
6.6	INCARICATI DEL TRATTAMENTO DEI DATI PERSONALI	13
6.7	ORGANIGRAMMA DELLE MANSIONI E RESPONSABILITA'	17
7	ANALISI DEI RISCHI	18
7.1	ANALISI DEI RISCHI SUI LUOGHI FISICI	19
7.2	ANALISI DEI RISCHI SULLE RISORSE HARDWARE	22
7.3	ANALISI DEI RISCHI SULLE RISORSE DATI	23
7.4	ANALISI DEI RISCHI SULLE RISORSE SOFTWARE	27
7.5	ANALISI DEI RISCHI SULL'ARCHIVIAZIONE DI TIPO CARTACEO	27
8	MISURE DI CONTROLLO DEI RISCHI	29
8.1	MISURE DI SICUREZZA FISICHE	32
8.2	MISURE DI SICUREZZA LOGICHE	33
8.3	MISURE DI SICUREZZA PROCEDURALE	34

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Titolare del ISTITUTO DI ISTRUZIONE SUPERIORE "PRIMO LEVI" Art. 34 D.Lgs
Trattamento: DIRIGENTE SCOLASTICO PROF. LAMBERTO PILLONETTO n. 196/2003

9	PIANO DI AUTOCONTROLLO ADOTTATO	35
10	CRITERI DI RIPRISTINO DATI DANNEGGIATI	36
11	PIANO DI FORMAZIONE DEGLI INCARICATI.....	36
12	DATI AFFIDATI ALL'ESTERNO DELLA STRUTTURA	37
13	CIFRATURA DEI DATI RELATIVI ALLO STATO DI SALUTE.....	37
14	REVISIONE DEL DOCUMENTO	38

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Titolare del **ISTITUTO DI ISTRUZIONE SUPERIORE "PRIMO LEVI"** **Art. 34 D.Lgs**
Trattamento: **DIRIGENTE SCOLASTICO PROF. LAMBERTO PILLONETTO** **n. 196/2003**

1 **SCOPO E AMBITO DI APPLICAZIONE DEL D.P.S.**

Il presente Documento Programmatico sulla Sicurezza (definito anche DPS) è adottato ai sensi delle disposizioni di cui all'art. 34 del Decreto Legislativo n. 196 del 30 giugno 2003, pubblicato in Gazzetta Ufficiale n. 174 il 29 luglio 2003. Nei modi previsti dall'Allegato B, Disciplinare Tecnico in materia di misure minime di sicurezza, questo documento definisce le politiche di sicurezza in materia di trattamento di dati personali, nonché i criteri tecnico-organizzativi per la loro attuazione.

Il Documento Programmatico sulla Sicurezza fornisce idonee informazioni relative al trattamento dei dati personali, sia che essi siano sensibili, giudiziari o comuni.

Il Documento Programmatico sulla Sicurezza, inoltre, riguarda il trattamento dei dati personali sia mediante strumenti elettronici di elaborazione sia mediante altri strumenti (cartacei, audio, visivi, etc.).

Questo obbligo di Legge ha portato a definire una metodologia aziendale che ha permesso, non solo di promuovere una reale cultura della protezione dei dati, ma anche di salvaguardare il patrimonio aziendale, costituito appunto dalle informazioni in nostro possesso, e di prendere altresì consapevolezza che la cultura della protezione dei dati non può che passare attraverso il ruolo fondamentale della formazione del personale.

Nel presente documento e nei relativi allegati i termini Trattamento, Dato personale, Dati identificativi, Dati sensibili, Dati giudiziari, Titolare, Responsabile, Incaricato, Interessato, Diffusione, Banca dati e tutti gli altri termini sono usati in conformità alle definizioni elencate all'art. 4 dello stesso Decreto Legislativo allegato al seguente documento.

Gli allegati alla presente documentazione costituiscono parte integrante del Documento Programmatico sulla Sicurezza dei dati.

2 **OBBLIGO DI LEGGE: REDAZIONE DEL DOCUMENTO**

L'obbligo della redazione di tale Documento Programmatico Sulla Sicurezza deriva dall'allegato B del D.Lgs. 196/2003 "DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA":

".....il titolare , .. redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:

- *l'elenco dei trattamenti di dati personali;*
- *la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;*
- *l'analisi dei rischi che incombono sui dati;*
- *le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;*
- *la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento...;*
- *la previsione di interventi formativi degli incaricati del trattamento, per render li edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei*

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Titolare del **ISTITUTO DI ISTRUZIONE SUPERIORE "PRIMO LEVI"** **Art. 34 D.Lgs**
Trattamento: **DIRIGENTE SCOLASTICO PROF. LAMBERTO PILLONETTO** **n. 196/2003**

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, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;

- *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;*
- *per i dati personali idonei a rivelare lo stato di salute e la vita sessuale .. " /individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato."*

Il documento procede innanzitutto dalla Identificazione delle Risorse da proteggere, risorse che in diverso modo operano o comunque svolgono un ruolo significativo nei processi di trattamento dei dati personali. A questo proposito, tramite l'Analisi dei Rischi, sono state analizzate le minacce e le vulnerabilità a cui tali risorse sono sottoposte, in modo da potere valutare gli elementi che possono insidiare la protezione, l'integrità, la conservazione di ogni singolo dato personale trattato.

Valutati i rischi, si è redatto un Piano di Sicurezza, tramite il quale si è provveduto a definire l'insieme delle misure fisiche, logiche ed organizzative adottate per tutelare le strutture e le risorse preposte al trattamento dati e quindi ai dati stessi.

Inoltre è stato definito un Piano di Verifiche delle misure adottate tramite il quale si provvederà ad accertare periodicamente la bontà delle misure individuate e ad apportare gli accorgimenti che si riveleranno necessari.

3 REVISIONI

La tabella sottostante riporta l'elenco delle revisioni a cui è stato sottoposto il presente Documento:

Rev. Nr.	Data	Descrizione intervento	Redatto da:	Approvato da:
0.0	31/03/2006	Prima stesura del documento	Dirigente Scolastico	Consiglio di Istituto

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Titolare del **ISTITUTO DI ISTRUZIONE SUPERIORE "PRIMO LEVI"** **Art. 34 D.Lgs**
Trattamento: **DIRIGENTE SCOLASTICO PROF. LAMBERTO PILLONETTO** **n. 196/2003**

4 DEFINIZIONI

TRATTAMENTO	qualsunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modifica, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca dati
DATO PERSONALE	qualsunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale
DATI IDENTIFICATIVI	i dati personali che permettono l'identificazione diretta dell'interessato
DATI SENSIBILI	i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute o la vita sessuale
DATI GIUDIZIARI	i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale
TITOLARE	la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza
RESPONSABILE	la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali
INCARICATI	le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile
INTERESSATO	la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali
COMUNICAZIONE	il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione
DIFFUSIONE	il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione
DATO ANONIMO	il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile
BLOCCO	la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Titolare del **ISTITUTO DI ISTRUZIONE SUPERIORE "PRIMO LEVI"** **Art. 34 D.Lgs**
Trattamento: **DIRIGENTE SCOLASTICO PROF. LAMBERTO PILLONETTO** **n. 196/2003**

BANCA DI DATI	Qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti
GARANTE	l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675
COMUNICAZIONE ELETTRONICA	ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile
CHIAMATA	la connessione istituita da un servizio telefonico accessibile al pubblico, che consente la comunicazione bidirezionale in tempo reale
RETI DI COMUNICAZIONE ELETTRONICA	i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportata
RETE PUBBLICA DI COMUNICAZIONE	una rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico
SERVIZIO DI COMUNICAZIONE ELETTRONICA	i servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazione e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, nei limiti previsti dall'articolo 2, lettera c), della direttiva 2002/21/CE del Parlamento Europeo e del Consiglio, del 7 marzo 2002
ABBONATO	qualunque persona fisica, persona giuridica, ente o associazione parte di un contratto con un fornitore di servizi di comunicazione elettronica accessibili al pubblico per la fornitura di tali servizi, o comunque destinatario di tali servizi tramite schede prepagate
UTENTE	qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata
DATI RELATIVI AL TRAFFICO	qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete elettronica o della relativa fatturazione
DATI RELATIVI ALL'UBICAZIONE	ogni dato trattato in una rete di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico
SERVIZIO A VALORE AGGIUNTO	il servizio che richiede il trattamento dei dati relativi al traffico o dei dati relativi all'ubicazione diversi dai dati relativi al traffico, oltre a quanto è necessario per la trasmissione di una comunicazione o della relativa fatturazione

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Titolare del **ISTITUTO DI ISTRUZIONE SUPERIORE "PRIMO LEVI"** **Art. 34 D.Lgs**
Trattamento: **DIRIGENTE SCOLASTICO PROF. LAMBERTO PILLONETTO** **n. 196/2003**

6 FIGURE PREVISTE PER LA SICUREZZA DEI DATI PERSONALI

6.1 TITOLARE DEL TRATTAMENTO DEI DATI PERSONALI

Il TITOLARE DEL TRATTAMENTO è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Il TITOLARE DEL TRATTAMENTO deve assicurare e garantire direttamente che vengano adottate le misure di sicurezza ai sensi del Codice in materia di Dati Personali tese a ridurre al minimo il rischio di distruzione dei dati, accesso non autorizzato o trattamento non consentito, previa idonee istruzioni fornite per iscritto.

Il TITOLARE DEL TRATTAMENTO, in relazione all'attività svolta, può individuare, nominare e incaricare per iscritto, se lo ritiene opportuno uno o più Responsabili della Sicurezza dei dati che assicurino e garantiscano che vengano adottate le misure di sicurezza ai sensi del Codice in materia di Dati Personali.

Qualora il Titolare del trattamento ritenga di non nominare alcun Responsabile della sicurezza dei dati, ne assumerà tutte le responsabilità e funzioni.

IL TITOLARE DEL TRATTAMENTO DEI DATI PERSONALI E':

IL DIRIGENTE SCOLASTICO: prof. Lamberto Pillonetto

6.2 RESPONSABILE DELLA SICUREZZA E DEL TRATTAMENTO DEI DATI PERSONALI

Il RESPONSABILE DELLA SICUREZZA E DEL TRATTAMENTO DEI DATI PERSONALI è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.

E' compito del Responsabile di cui sopra:

- Nominare gli incaricati del trattamento per le banche dati che gli sono state affidate;
- Di sorvegliare che il trattamento sia effettuato nei termini e nei modi stabiliti dal Codice in materia di dati personali;
- Di dare istruzioni adeguate agli incaricati del trattamento effettuato con strumenti elettronici e non;
- Periodicamente, e comunque almeno annualmente, verifica la sussistenza delle condizioni per la conservazione dei profili di autorizzazione degli incaricati del trattamento dei dati personali.

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Titolare del **ISTITUTO DI ISTRUZIONE SUPERIORE "PRIMO LEVI"** **Art. 34 D.Lgs**
Trattamento: **DIRIGENTE SCOLASTICO PROF. LAMBERTO PILLONETTO** **n. 196/2003**

Qualora il Titolare del trattamento ritenga di non nominare alcun Responsabile della sicurezza e del trattamento dei dati, ne assumerà tutte le responsabilità e funzioni.

La nomina di ciascun Responsabile della Sicurezza e del Trattamento dei dati personali è effettuata dal Titolare del Trattamento con lettera d'incarico [vd. *Allegato - rif. R_SDP*] in cui sono specificate le responsabilità che gli sono affidate. Tale lettera sarà controfirmata dall'interessato per accettazione.

Copia della lettera di nomina accettata è conservata dal Titolare del trattamento in **LUOGO SICURO**.

Tale nomina è a TEMPO INDETERMINATO e decade per revoca o dimissioni dello stesso.

La nomina del RESPONSABILE DELLA SICUREZZA E DEL TRATTAMENTO DEI DATI PERSONALI può essere revocata in qualsiasi momento dal TITOLARE DEL TRATTAMENTO DEI DATI **SENZA PREAVVISO**, ed eventualmente affidata ad altro soggetto.

IL RESPONSABILE DELLA SICUREZZA E DEL TRATTAMENTO DEI DATI PERSONALI

E':

IL DIRETTORE dei S.G.A.: sig. ra Pepe Maria

Lettera di nomina n. 5556/C1 del 04/10/2005

6.3 RESPONSABILITÀ DELLA GESTIONE E MANUTENZIONE DEGLI STRUMENTI ELETTRONICI

IL RESPONSABILE DELLA GESTIONE E MANUTENZIONE DEGLI STRUMENTI ELETTRONICI è la persona fisica, la persona giuridica e qualsiasi altro ente, associazione od organismo che sovrintende alle risorse del sistema operativo di un elaboratore o di un sistema di Banche di dati.

E' compito del RESPONSABILE DELLA GESTIONE E MANUTENZIONE DEGLI STRUMENTI ELETTRONICI:

- Attivare le credenziali di autenticazione (password) agli incaricati del trattamento, su indicazione del RESPONSABILE DEL TRATTAMENTO, per tutti i trattamenti effettuati con strumenti informatici;
- Definire quali politiche adottare per la protezione dei sistemi contro i virus informatici e verificarne l'efficacia con cadenza almeno semestrale;
- Proteggere gli elaboratori dal rischio di intrusione [violazione da parte degli "hackers"];
- Informare il RESPONSABILE DELLA SICUREZZA DEI DATI PERSONALI nella eventualità

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Titolare del **ISTITUTO DI ISTRUZIONE SUPERIORE "PRIMO LEVI"** **Art. 34 D.Lgs**
Trattamento: **DIRIGENTE SCOLASTICO PROF. LAMBERTO PILLONETTO** **n. 196/2003**

che si siano rilevati dei rischi relativamente alle misure di sicurezza riguardanti i dati personali.

Qualora il Responsabile della sicurezza dei dati personali ritenga di non nominare alcun Responsabile della gestione e della manutenzione degli strumenti elettronici, ne assumerà tutte le responsabilità e funzioni.

La nomina di ciascun Responsabile della gestione e della manutenzione degli strumenti elettronici è effettuata dal Titolare del trattamento dei dati personali con una lettera d'incarico [vd. *Allegati - rif. R_GMSE*] in cui sono specificate le responsabilità che gli sono affidate. Tale lettera sarà controfirmata dall'interessato per accettazione.

Copia della lettera di nomina accettata è conservata dal Responsabile della sicurezza dei dati personali in LUOGO SICURO.

Tale nomina è a TEMPO INDETERMINATO e decade per revoca o dimissioni dello stesso.

La nomina del RESPONSABILE DELLA GESTIONE E MANUTENZIONE DEGLI STRUMENTI ELETTRONICI può essere revocata in qualsiasi momento dal TITOLARE DEL TRATTAMENTO DEI DATI PERSONALI **SENZA PREAVVISO**, ed eventualmente affidata ad altro soggetto.

IL RESPONSABILE DELLA GESTIONE E MANUTENZIONE DEGLI STRUMENTI ELETTRONICI NEI LABORATORI DI INFORMATICA E':

L'ASSISTENTE TECNICO: sig. Da Parè Tiziano

Lettera di nomina n. 2361/C1 del **28/03/2006**

IL RESPONSABILE DELLA GESTIONE E MANUTENZIONE DEGLI STRUMENTI ELETTRONICI NEGLI UFFICI DI SEGRETERIA, PRESIDENZA E SALA INSEGNANTI E':

L'ASSISTENTE TECNICO: sig. Bergamo Elio

Lettera di nomina n. /C1 del **31/03/2006**

6.4 INCARICATO DELLA CUSTODIA DELLE COPIE DELLE CREDENZIALI

IL RESPONSABILE DELLA SICUREZZA DEI DATI PERSONALI può individuare, nominare ed incaricare per iscritto, SE LO RITIENE OPPORTUNO, uno o più INCARICATI DELLA CUSTODIA DELLE COPIE DELLE CREDENZIALI.

E' compito degli incaricati di cui sopra:

- Gestire e custodire le credenziali per l'accesso ai dati degli incaricati del trattamento;

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Titolare del **ISTITUTO DI ISTRUZIONE SUPERIORE "PRIMO LEVI"** **Art. 34 D.Lgs**
Trattamento: **DIRIGENTE SCOLASTICO PROF. LAMBERTO PILLONETTO** **n. 196/2003**

- Predisporre, per ogni incaricato del trattamento, una busta sulla quale è indicato il nome dell'incaricato e all'interno della busta deve essere indicata la credenziale usata. Le buste con le credenziali sono conservate dal Responsabile della sicurezza dei dati personali in **LUOGO SICURO**;
- Istruire gli incaricati del trattamento sull'uso delle parole chiave, e sulle caratteristiche che debbono avere, e sulle modalità per la loro modifica in autonomia;
- Revocare tutte le credenziali non utilizzate in caso di perdita della qualità che consentiva all'incaricato l'accesso ai dati personali;
- Revocare le credenziali per l'accesso ai dati degli **INCARICATI DEL TRATTAMENTO** nel caso di mancato utilizzo per oltre **SEI MESI**.

Qualora il Responsabile della sicurezza dei dati personali ritenga di non nominare alcun Incaricato della custodia delle copie delle credenziali, ne assumerà tutte le responsabilità e funzioni.

La nomina di ciascun Incaricato della custodia delle copie delle credenziali è effettuata dal Responsabile della sicurezza dei dati personali con una lettera d'incarico [vd. *Allegati - rif. R_CCC*] in cui sono specificate le responsabilità che gli sono affidate. Tale lettera sarà controfirmata dall'interessato per accettazione.

Copia della lettera di nomina accettata è conservata dal Responsabile della sicurezza dei dati personali in **LUOGO SICURO**.

Tale nomina è a TEMPO INDETERMINATO e decade per revoca o dimissioni dello stesso.

La nomina degli **INCARICATI DELLA CUSTODIA DELLE COPIE DELLE CREDENZIALI** può essere revocata in qualsiasi momento dal **RESPONSABILE DELLA SICUREZZA DEI DATI PERSONALI SENZA PREAVVISO**, ed eventualmente affidata ad altro soggetto.

L'INCARICATO DELLA GESTIONE DELLE CREDENZIALI E':

L'ASSISTENTE AMMINISTRATIVO: sig.ra Facchin Fabiola

Lettera di nomina n. 2362/C1 del 28/03/2006

6.5 INCARICATO DELLE COPIE DI SICUREZZA DELLE BANCHE DATI

Il **RESPONSABILE DELLA SICUREZZA DEI DATI PERSONALI** può individuare, nominare ed incaricare per iscritto, **SE LO RITIENE OPPORTUNO**, uno o più **INCARICATI DELLE COPIE DI SICUREZZA DELLE BANCHE DATI**.

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Titolare del **ISTITUTO DI ISTRUZIONE SUPERIORE "PRIMO LEVI"** **Art. 34 D.Lgs**
Trattamento: **DIRIGENTE SCOLASTICO PROF. LAMBERTO PILLONETTO** **n. 196/2003**

Tale figura ha il compito di effettuare periodicamente le copie di sicurezza delle Banche di dati gestite.

E' compito degli incaricati di cui sopra:

- Prendere tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvedere al ricovero periodico degli stessi con copie di sicurezza secondo i criteri stabiliti dal RESPONSABILE DELLA SICUREZZA DEI DATI PERSONALI;
- Assicurarsi della qualità delle copie di sicurezza dei dati e della loro conservazione in luogo adatto, sicuro e ad accesso controllato;
- Di provvedere a conservare con la massima cura e custodia i dispositivi utilizzati per le copie di sicurezza, impedendo l'accesso agli stessi dispositivi da parte di personale non autorizzato;
- Di segnalare tempestivamente al responsabile della gestione e della manutenzione degli strumenti elettronici, ogni eventuale problema dovesse verificarsi nella normale attività di copia delle banche dati.

Qualora il Responsabile della sicurezza dei dati personali ritenga di non nominare alcun Incaricato delle copie di sicurezza delle banche dati, ne assumerà tutte le responsabilità e funzioni.

La nomina di ciascun Incaricato delle copie di sicurezza delle banche dati è effettuata dal Responsabile della sicurezza dei dati personali con una lettera d'incarico [vd. *Allegati - rif. R_CSBD*] in cui sono specificate le responsabilità che gli sono affidate. Tale lettera sarà controfirmata dall'interessato per accettazione.

Copia della lettera di nomina accettata è conservata dal Responsabile della sicurezza dei dati personali in LUOGO SICURO.

Tale nomina è a TEMPO INDETERMINATO e decade per revoca o dimissioni dello stesso.

La nomina degli INCARICATI DELLA CUSTODIA DELLE COPIE DI SICUREZZA DELLE BANCHE DATI può essere revocata in qualsiasi momento dal RESPONSABILE DELLA SICUREZZA DEI DATI PERSONALI **SENZA PREAVVISO**, ed eventualmente affidata ad altro soggetto.

L'INCARICATO DELLA SICUREZZA DELLE BANCHE DATI E':

L'ASSISTENTE AMMINISTRATIVO: sig. Piva Roberto

Lettera di nomina n. 2363/C4 del 28/03/2006

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Titolare del **ISTITUTO DI ISTRUZIONE SUPERIORE "PRIMO LEVI"** **Art. 34 D.Lgs**
Trattamento: **DIRIGENTE SCOLASTICO PROF. LAMBERTO PILLONETTO** **n. 196/2003**

6.6 INCARICATI DEL TRATTAMENTO DEI DATI PERSONALI

Il RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI può individuare, nominare ed incaricare per iscritto, SE LO RITIENE OPPORTUNO, uno o più INCARICATI DEL TRATTAMENTO DEI DATI PERSONALI.

E' compito degli incaricati di cui sopra osservare le seguenti disposizioni:

- Gli incaricati che hanno ricevuto credenziali di autenticazione per il trattamento dei dati personali, debbono conservare con la massima segretezza le parole chiave e i dispositivi di autenticazione in loro possesso e uso esclusivo;
- La parola chiave, quando è prevista dal sistema di autenticazione, deve essere 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;
- La parola chiave non deve contenere riferimenti agevolmente riconducibili all'incaricato;
- L'incaricato del trattamento deve modificarla al primo utilizzo e, successivamente, almeno OGNI SEI MESI;
- In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave deve essere modificata almeno OGNI TRE MESI;
- Gli incaricati del trattamento non debbono in nessun caso lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento dei dati personali;
- Gli incaricati del trattamento debbono controllare e custodire, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti contenenti dati personali;
- 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.

Qualora il Responsabile del trattamento dei dati personali ritenga di non nominare alcun Incaricato del trattamento dei dati personali, ne assumerà tutte le responsabilità e funzioni.

La nomina di ciascun Incaricato del trattamento dei dati personali è effettuata dal Responsabile del trattamento dei dati personali con una lettera d'incarico [vd. *Allegati - rif. 1_TOP*] in cui sono specificate le responsabilità che gli sono affidate. Tale lettera sarà controfirmata dall'interessato per accettazione.

Copia della lettera di nomina accettata è conservata dal Responsabile del trattamento dei dati personali in LUOGO SICURO.

Tale nomina è a TEMPO INDETERMINATO e decade per revoca o dimissioni dello

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Titolare del **ISTITUTO DI ISTRUZIONE SUPERIORE "PRIMO LEVI"** **Art. 34 D.Lgs**
Trattamento: **DIRIGENTE SCOLASTICO PROF. LAMBERTO PILLONETTO** **n. 196/2003**

stesso.

Agli INCARICATI DEL TRATTAMENTO DEI DATI PERSONALI è assegnata una **parola chiave** e un **codice di autenticazione informatica**.

Agli INCARICATI DEL TRATTAMENTO DEI DATI PERSONALI è prescritto di adottare le necessarie cautele per assicurare la segretezza della **parola chiave** e la diligente custodia dei dispositivi in possesso e ad uso esclusivo dell'incaricato.

La nomina degli INCARICATI DEL TRATTAMENTO DEI DATI PERSONALI può essere revocata in qualsiasi momento dal RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI **SENZA PREAVVISO**, ed eventualmente affidata ad altro soggetto.

GLI INCARICATI DEL TRATTAMENTO DEI DATI PERSONALI SONO:

DOCENTI:

ACQUAVIVA	ENRICO
ALFIERI	SANTINA
ANDOLFATO	FRANCESCO
ARBIA	ALDO
ARENA	LUISA
ASSOM	MARIALUISA
BACCIN	MARIA CATERINA
BALDASSO	DINO
BASURTO	MASSIMO
BELLAN	FRANCESCA
BELLERO	ANTONELLA
BERGAMIN	GIOVANNI
BERTI	CATIA
BESAZZA	EVA
BILLE'	ANTONIA
BOERIO	MARCO
BOLZONELLO	SUSANNA
BONECHI	LORENZO
BONESSO	PATRIZIA
BONORA	DANILO
BORDIN	CRISTINA
BREDA	GIORDANA
CANINO	GIUSEPPE
CANNATA	MICHELA
CATTELAN	GIULIA
CELOTTO	AMALIA
CERON	ANGELO
CICCONE	NATALIA

ASSISTENTI AMMINISTRATIVI:

BISOL	GIOVANNA
BORDONARO	SONIA
CALABRESE	MIRANGELA
CANEVESE	MICHELA
FACCHIN	FABIOLA
FELTRIN	ALESSANDRA
PIVA	ROBERTO
RUZZA	MICHELA
SECCO	LORETTA

ASSISTENTI TECNICI:

BONORA	MARIO
BERGAMO	ELIO
DA PARE'	TIZIANO
GIUFFRIDA	GIUSEPPE

COLLABORATORI SCOLASTICI

BARBISAN	MARIA
BASEGGIO	ALMA
BERNO	ANTONIO
BONESSO	ELISABETTA
CARBE'	ANNA
GASPARETTO	ANNA
GAZZILLO	DOMENICO
MARTIGNAGO	GIUSEPPE
MARTIGNAGO	RENATO

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Titolare del **ISTITUTO DI ISTRUZIONE SUPERIORE "PRIMO LEVI"** **Art. 34 D.Lgs**
Trattamento: **DIRIGENTE SCOLASTICO PROF. LAMBERTO PILLONETTO** **n. 196/2003**

CIMA	LUIGI	PANDOLFO	AMABILE
CIMOLATO	MICHELE	PELLIZZARI	RAFFAELE
CITERONI	RAFFAELLA	RENOSTO	MARIA GRAZIA
COSTENIERO	EVA	RIZZOTTO	OLGA
CUSINATO	BRUNA	SAVI	GIACOMO
DAL CANTON	SILVIA	ZANIOL	BRUNO
DAL PICCOL	MICHELA		
DALL'OGGIO	ANTONELLA		
DE LUCCHI	DINA		
DEL PRETE	ELENA		
DI PREMIO	GIULIANA		
FABRICI	MARIA SANTA		
FLORA	GIUSEPPE		
FONTE BASSO	CHIARA		
FORNASIERO	MATTEO		
FURLANETTO	PIETRO		
FURLANETTO	VALERIO		
GALLI	DONATELLA		
GIANSANTE	GIUSEPPE		
GUIDA	ANGELO		
IAZZETTA	VIRGINIA NATALIA		
IMPERATO	PAOLO		
LABATE	GIUSEPPINA		
LENZO	GRAZIELLA		
LICCIARDI	MARIA		
LICITRA	GIOVANNA		
MAGGIO	ELENA MARIA		
MALAGUTI	PAOLO		
MANESSO	AMERIGO		
MARAZZATO	ROBERTO		
MARIUZ	RENATO		
MAZZARO	STEFANO		
MELLUSO	VITTORIA		
MERLO	IVO		
MORELLATO	CLAUDIO		
NAPOLITANO	MARIA		
NUBILE	GIOVANNI		
PADOVAN	NICOLETTA		
PANTANO	SILVANA		
PASA	LAURA		
PATRICELLI	DOROTEA		
PATUZZO	MONICA		
PAVAN	LUCIO		
PAVARIN	BIANCA		
PEDRINI	ROSSELLA		

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Titolare del **ISTITUTO DI ISTRUZIONE SUPERIORE "PRIMO LEVI"** **Art. 34 D.Lgs**
Trattamento: **DIRIGENTE SCOLASTICO PROF. LAMBERTO PILLONETTO** **n. 196/2003**

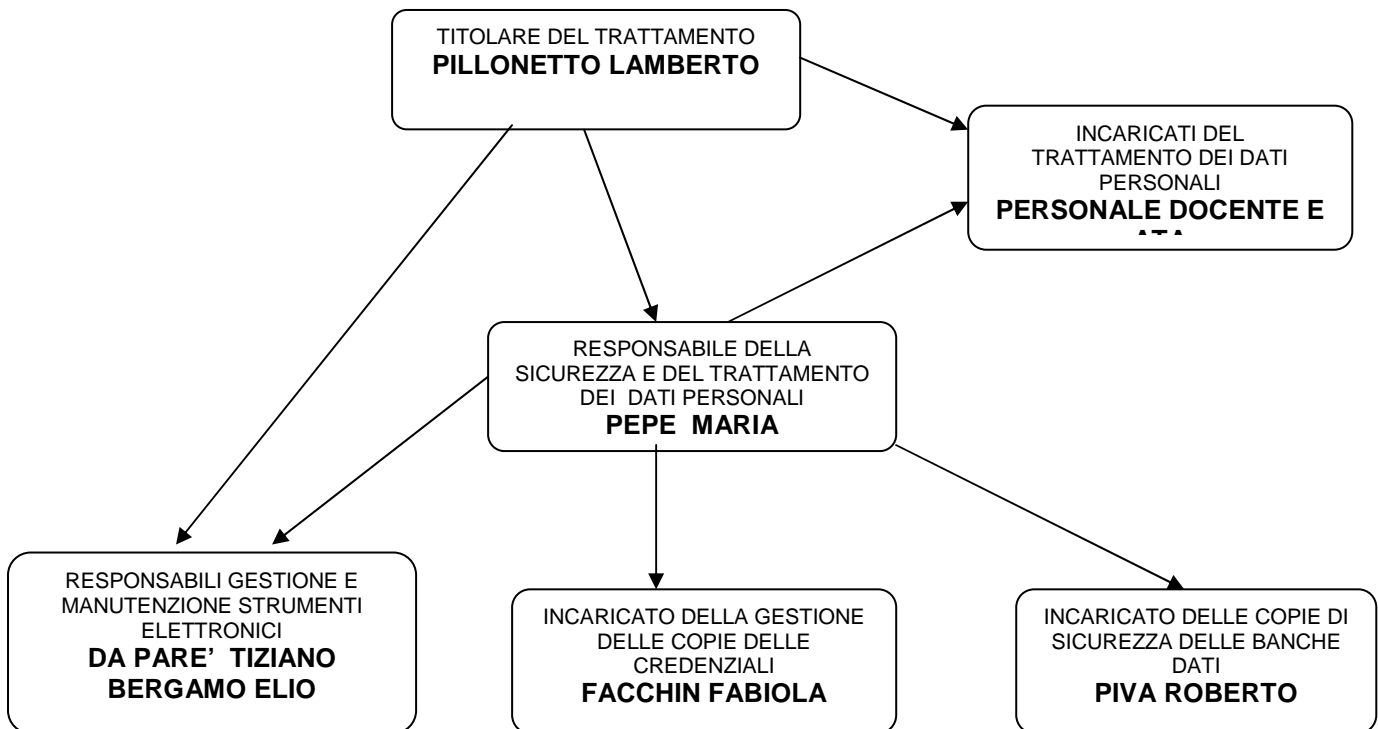
PERINOT	CLAUDIO
PIVATO	ALBERTO
PIZZOLO	ANNA
POGGI	PAOLO
POLETTI	ENNIO
POLONI	ANTONELLA
PONTANI	FILIPPOMARIA
PUGLIESE	MARIA ROSARIA
QUAGGIOTTO	NADIA
QUAGGIOTTO	VITTORIO
RAGAGNIN	RUGGERO
RAMAZZINA	ERMANNIO
RAMON	SERGIO
RIONDATO	EMILY
RUPERTI	ROSA ANNA
SABATO	ALFREDO
SACCONI	MARIA
SANTIN	ROBERTA
SARTOR	DONELLA
SARTORI	LINO
SARTORI	MARIA GIOVANNA
SCANFERLA	MASSIMO
SEVERIN	ORNELLA
SOLITRO	ANNA
SOTGIU	IOLANDA
SPADA	EMANUELE
STABENE	ILVIA
STOCCO	ANGELA
SUSIN	DANIELA
TESTA	FEDERICO
TRACINA'	ANTONELLA
TRENTIN	ERNESTINA
TRONCHIN	DANIELA
URSO	MILENA
VANIN	GABRIELE
VISENTIN	FANIO
VIVIANI	ELISA
VIZZINO	GIUSEPPE
ZAMBET	CLAUDIA
ZAMPIERI	FRANCESCO
ZORZI	ALESSANDRO

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Titolare del **ISTITUTO DI ISTRUZIONE SUPERIORE "PRIMO LEVI"**
Trattamento: **DIRIGENTE SCOLASTICO PROF. LAMBERTO PILLONETTO**

Art. 34 D.Lgs
n. 196/2003

6.7 ORGANIGRAMMA DELLE MANSIONI E RESPONSABILITA'



DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Titolare del **ISTITUTO DI ISTRUZIONE SUPERIORE “PRIMO LEVI”** **Art. 34 D.Lgs**
Trattamento: **DIRIGENTE SCOLASTICO PROF. LAMBERTO PILLONETTO** **n. 196/2003**

7 ANALISI DEI RISCHI

Questo capitolo contiene i rischi legati al trattamento di dati personali secondo le categorie di rischio elencate nell'articolo 31 del codice:

Art. 31 – (Obblighi di sicurezza): I dati personali oggetto di trattamento sono 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.

I rischi che vengono presi in considerazione sono di due tipi, a seconda che riguardino il rispetto del codice della privacy, oppure i rischi propri di un sistema informativo.

L'analisi di rischio è stata articolata in due parti:

- 1 Una parte che identifica, valuta e contrasta i rischi indicati dalla legge, e cioè "il rischio 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";
- 2 Una parte che identifica, valuta e contrasta i rischi individuati dal gestore del sistema informativo, che sono propri della sua attività.

L'analisi svolta ha compreso le seguenti categorie di rischio:

- 1 Analisi dei rischi sui luoghi fisici;
- 2 Analisi dei rischi sulle risorse hardware;
- 3 Analisi dei rischi sulle risorse dati;
- 4 Analisi dei rischi sulle risorse software;
- 5 Analisi dei rischi sull'archiviazione di tipo cartaceo.

E' possibile quantificare il rischio ed ottenere così degli indici di priorità di intervento.

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Titolare del **ISTITUTO DI ISTRUZIONE SUPERIORE "PRIMO LEVI"** **Art. 34 D.Lgs**
Trattamento: **DIRIGENTE SCOLASTICO PROF. LAMBERTO PILLONETTO** **n. 196/2003**

SOGLIA DI RISCHIO	DESCRIZIONE DEL RISCHIO
LIEVE	Con questa soglia viene individuato un rischio molto basso, che identifica una minaccia remota, in ogni caso rapidamente reversibile od ovviabile.
BASSA	Con questa soglia viene individuato un rischio di tipo superiore al precedente, ma non irreversibile.
MEDIA	Con questa soglia viene individuato un rischio di tipo superiore al precedente, identificante una minaccia remota, ma i cui effetti non sono totalmente oppure parzialmente reversibili od ovviabili. In tale caso è già consigliabile pensare ad opportuni accorgimenti per contenere il rischio.
GRAVE O GRAVISSIMA	Con queste soglie vengono individuati rischi che è sicuramente inaccettabile pensare di correre. Pertanto dovrà sicuramente essere attivato un insieme di contromisure (di natura fisica, logica etc.) per abbattere il rischio e contenerlo in livelli accettabili.

7.1 ANALISI DEI RISCHI SUI LUOGHI FISICI

I locali dove vengono trattati dati personali, sia per mezzo di documenti cartacei che attraverso applicazioni ed archivi informatici, sono situati all'interno degli uffici.

L'accesso ai locali è consentito solo al personale dipendente, ed è sottoposto al controllo degli addetti al ricevimento. Gli utenti esterni (alunni genitori ed altro personale) non entrano all'interno degli uffici se non accompagnati da personale dipendente.

Nell'Ufficio del Dirigente Scolastico gli utenti esterni (alunni e genitori) possono sostare solo in prossimità della scrivania. Non vengono in contatto con nessun tipo di documento cartaceo e/o informatico.

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Titolare del **ISTITUTO DI ISTRUZIONE SUPERIORE "PRIMO LEVI"** **Art. 34 D.Lgs**
Trattamento: **DIRIGENTE SCOLASTICO PROF. LAMBERTO PILLONETTO** **n. 196/2003**

UFFICI – ORARI DI ACCESSO AL PUBBLICO

Negli uffici l'accesso al pubblico avviene secondo degli orari prestabiliti:

D.S.G.A.: Tutti i giorni dalle 8.00 alle 13.00;

UFFICIO PROTOCOLLO: Tutti i giorni dalle 10.00 alle 12.00;

UFFICIO ALUNNI: Dal Lunedì al Sabato dalle 7.30 alle 7.50 e dalle 10.30 alle 13.30;
Il Lunedì dalle 15.30 alle 17.30;

UFFICIO AMMINISTRATIVO: Dal Lunedì al Sabato dalle 10.00 alle 12.00;
Il Mercoledì dalle 15.30 alle 17.30;

UFFICI - LOGISTICA

PRESENZA DI ARMADI BLINDATI : SI

PRESENZA DI ARMADI IGNIFUGHI: NO

PRESENZA DI ARMADI CON SERRATURA: SI

PRESENZA DI ARMADI SENZA SERRATURA: NO

PRESENZA DI SCAFFALATURE: SI

PORTE CON CHIUSURA A CHIAVE: SI

PORTE SENZA CHIUSURA A CHIAVE: NO

PORTE AD APERTURA AUTOMATICA: NO

FINESTRE CON INFERRIATE: NO

MEZZI DI ESTINZIONE ANTINCENDIO: SI

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Titolare del **ISTITUTO DI ISTRUZIONE SUPERIORE “PRIMO LEVI”** **Art. 34 D.Lgs**
Trattamento: **DIRIGENTE SCOLASTICO PROF. LAMBERTO PILLONETTO** **n. 196/2003**

All'interno degli uffici sono presenti armadi contenenti sia dati identificativi sia dati non rientranti nel campo di applicazione della presente normativa.

Gli elaboratori sono tutti situati all'interno di locali protetti da porte dotate di serratura.

L'accesso è consentito solo al personale autorizzato.

I locali interessati dalle misure di sicurezza sono dotati di attrezzature antincendio (mezzi di estinzione a polvere ed anidride carbonica omologati) in manutenzione ordinaria da parte di una società specializzata.

La manutenzione periodica è effettuata da una ditta specializzata.

All'interno dell'Ufficio del Dirigente Scolastico sono presenti armadi contenenti sia dati identificativi sia dati non rientranti nel campo di applicazione della presente normativa.

L'accesso è consentito solo al personale autorizzato.

ELEMENTI DI RISCHIO E PRECAUZIONI ADOTTATE

ACCESSI NON AUTORIZZATI A LOCALI AD ACCESSO RISTRETTO – SOGLIA DI RISCHIO BASSA – Gli Uffici hanno un solo accesso sempre presidiato durante il normale svolgimento dell'attività lavorativa. Al di fuori dell'attività lavorativa i locali sono chiusi a chiave.

SOTTRAZIONE DI STRUMENTI CONTENENTI DATI – SOGLIA DI RISCHIO BASSA – Gli Uffici hanno un solo accesso sempre presidiato durante il normale svolgimento dell'attività lavorativa. Al di fuori dell'attività lavorativa i locali sono chiusi a chiave.

EVENTI DISTRUTTIVI, NATURALI O ARTIFICIALI (Movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali,...) – SOGLIA DI RISCHIO BASSA – L'impianto di messa a terra risulta installato a regola d'arte e sottoposto a regolare manutenzione. L'edificio risulta autoprotetto da scariche atmosferiche. Presenti sistemi di protezione antincendio. Area non soggetta ad allagamenti.

GUASTI AI SISTEMI COMPLEMENTARI (Impianto elettrico, ...) – **SOGLIA DI RISCHIO BASSA** – L'impianto elettrico risulta costruito a regola d'arte. E' presente la dichiarazione di conformità firmata dall'installatore.

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Titolare del **ISTITUTO DI ISTRUZIONE SUPERIORE "PRIMO LEVI"** **Art. 34 D.Lgs**
Trattamento: **DIRIGENTE SCOLASTICO PROF. LAMBERTO PILLONETTO** **n. 196/2003**

7.2 ANALISI DEI RISCHI SULLE RISORSE HARDWARE

All'interno dei locali descritti in precedenza sono presenti i seguenti mezzi elettronici:

- 1 Personal Computer Fissi
- 2 Personal Computer Portatili
- 3 Server

I Personal Computer risultano tutti sollevati da terra in modo da evitare perdite di dati dovuti ad allagamenti.

I Sistemi utilizzati presentano la possibilità di password di ingresso personalizzabili per cui sono soddisfatti i requisiti minimi imposti dalla normativa vigente.

Sono state nominate le persone cui è affidata la responsabilità tecnica di amministrare le apparecchiature e gli incaricati della custodia delle copie delle credenziali.

I Personal Computer sono dotati di dispositivi di lettura CD-ROM/DVD e alcuni anche di dispositivi per la masterizzazione.

I rischi analizzati sono i seguenti:

- 1 USO NON AUTORIZZATO DELL' HARDWARE
- 2 RIVELAZIONE (PER COMUNICAZIONE O DIFFUSIONE) ILLEGITTIMA DI INFORMAZIONI, ANCHE PER NEGLIGENZA
- 3 ALTERAZIONE NON AUTORIZZATA DI INFORMAZIONI
- 4 PERDITA DI INFORMAZIONI
- 5 USO NON AUTORIZZATO DI INFORMAZIONI E DI APPLICATIVI
- 6 PERDITA O RIUTILIZZO DI SUPPORTI CARTACEI O MAGNETICI E DOCUMENTAZIONI ACCESSORIE

ELEMENTI DI RISCHIO E PRECAUZIONI ADOTTATE

USO NON AUTORIZZATO DELL' HARDWARE – SOGLIA DI RISCHIO BASSA – L'utilizzo dell'hardware è soggetto all'utilizzo di password.

MANOMISSIONE E SABOTAGGIO – SOGLIA DI RISCHIO BASSA – Alle risorse non accedono persone non autorizzate. La manutenzione è effettuata da tecnici di fiducia.

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Titolare del **ISTITUTO DI ISTRUZIONE SUPERIORE "PRIMO LEVI"** **Art. 34 D.Lgs**
Trattamento: **DIRIGENTE SCOLASTICO PROF. LAMBERTO PILLONETTO** **n. 196/2003**

PROBABILITA' FREQUENZA DI GUASTO – SOGLIA DI RISCHIO BASSA – L'hardware è di qualità e storicamente non ha mai dato problemi rilevanti.

INTERCETTAZIONE DELLE TRASMISSIONI – SOGLIA DI RISCHIO BASSA - Protezione "firewall" su ogni Personal Computer.

RISCHI CONNESSI ALL'ELETTRICITA' – SOGLIA DI RISCHIO BASSA – Storicamente la zona in cui ha sede l'azienda non è a rischio elevato di black out. Tutte le risorse hardware sono collegate ad un server, che grazie ad un gruppo di continuità, consente di escludere la perdita di dati derivanti da sbalzi di tensione o da interruzioni improvvise di corrente elettrica.

7.3 ANALISI DEI RISCHI SULLE RISORSE DATI

DEFINIZIONE E UTILIZZO DEI CODICI IDENTIFICATIVI PERSONALI

Scopo dei codici identificativi personali è quello di consentire l'utilizzo degli strumenti elettronici solo alle persone che sono autorizzate dalla Società

I codici identificativi personali che danno accesso ai server vengono definiti ed attivati dal Responsabile della gestione e manutenzione degli strumenti elettronici e/o dall'Incaricato della custodia delle copie delle credenziali. I codici identificativi personali che danno accesso alle postazioni di lavoro e alla rete interna sono definiti ed attivati dal Responsabile della gestione e manutenzione degli strumenti elettronici e/o dall'Incaricato della custodia delle copie della credenziali, i quali sono gli unici depositari della conoscenza del sistema che consente la loro attivazione, rilevazione e modificazione.

DEFINIZIONE E UTILIZZO DELLA PAROLE CHIAVE

Scopo delle parole chiave è quello di consentire l'accesso alle applicazioni informatiche solo da parte delle persone che sono autorizzate dalla Società.

Le parole chiave vengono definite ed ufficializzate dal Responsabile della gestione e manutenzione degli strumenti elettronici e/o dall'Incaricato della custodia delle copie delle credenziali, i quali sono gli unici depositari della conoscenza e del sistema che consente l'attivazione, la rilevazione e la modificazione delle parole chiave.

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Titolare del **ISTITUTO DI ISTRUZIONE SUPERIORE "PRIMO LEVI"** **Art. 34 D.Lgs**
Trattamento: **DIRIGENTE SCOLASTICO PROF. LAMBERTO PILLONETTO** **n. 196/2003**

Le parole chiave vengono assegnate in maniera selettiva in funzione alle mansioni e alle responsabilità ricoperte da ciascun utente. Le parole chiave sono definite con modalità che variano a seconda dell'applicazione informatica cui danno accesso.

In linea generale esse sono definite inizialmente dal Responsabile della gestione e manutenzione degli strumenti elettronici e/o dall'Incaricato della custodia delle copie delle credenziali e, dopo la sua attivazione, direttamente dal singolo utente.

L'accesso alle applicazioni informatiche che consentono la gestione ed il trattamento di dati personali e ai relativi archivi può avvenire soltanto previa digitazione, nell'apposito campo della videata principale, della parola chiave, non visibile a terzi, in quanto mascherata da asterischi durante la sua digitazione.

I codici identificativi personali e le relative parole chiave che danno accesso alle varie applicazioni utente vengono definiti ed attivati dal Responsabile della gestione e manutenzione degli strumenti elettronici e/o dall'Incaricato della custodia delle copie delle credenziali. La sintassi del codice identificativo e della parola chiave dipendono dalle specifiche del prodotto applicativo.

SISTEMI DI SICUREZZA ED ARCHIVI MAGNETICI

Per evitare la perdita o la distruzione dei dati personali, il sistema informatico è dotato di un sistema di sicurezza, basato su procedure per la produzione di copie di salvataggio ("backup") degli archivi magnetici, contenenti i programmi applicativi di produzione, le librerie e gli archivi di dati e per il loro ripristino in caso di emergenza ("restore").

Le copie di sicurezza sono depositate in armadi dislocati presso la sede della Società.

Il backup complessivo dei principali dati è effettuato dal personale preposto ed autorizzato dal Titolare del trattamento.

DEFINIZIONE DEI COMPITI PER LA GESTIONE DEGLI ACCESSI AL SISTEMA INFORMATICO

L'accesso agli strumenti elettronici che costituiscono l'intero sistema informatico è consentito solo attraverso un codice identificativo personale, assegnato dal Responsabile della gestione e manutenzione degli strumenti elettronici e/o dall'Incaricato della custodia delle copie delle credenziali.

A costui sono stati attribuiti, con la lettera di nomina, specifici compiti e responsabilità per la definizione delle modalità di accesso e per evitare che le informazioni concernenti le parole chiave, i codici identificativi personali e le modalità per la loro definizione vengano a conoscenza di terzi non autorizzati.

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Titolare del **ISTITUTO DI ISTRUZIONE SUPERIORE "PRIMO LEVI"** **Art. 34 D.Lgs**
Trattamento: **DIRIGENTE SCOLASTICO PROF. LAMBERTO PILLONETTO** **n. 196/2003**

L'accesso alla rete interna, che consente, a sua volta, l'accesso alle applicazioni informatiche e agli archivi dei dati è consentito solo attraverso un "codice identificativo personale" e una "parola chiave", assegnati dal Responsabile della gestione e manutenzione degli strumenti elettronici e/o dall'Incaricato della custodia delle copie delle credenziali. A costui sono stati attribuiti, con la lettera di nomina, specifici compiti e responsabilità per la definizione delle modalità di accesso e per evitare che le informazioni che concernono le parole chiave, i codici identificativi personali e le modalità per la loro definizione vengano a conoscenza di terzi non autorizzati.

ELEMENTI DI RISCHIO E PRECAUZIONI ADOTTATE

ACCESSO NON AUTORIZZATO – SOGLIA DI RISCHIO BASSA – L'accesso alle risorse dati in formato elettronico avviene solo tramite gli elaboratori protetti da password e da software di crittografia dei dati. All'archivio cartaceo possono accedere solo i diretti incaricati.

CANCELLAZIONE NON AUTORIZZATA DI DATI/MANOMISSIONE DI DATI – SOGLIA DI RISCHIO BASSA – L'accesso agli elaboratori avviene solo tramite gli elaboratori protetti da password. All'archivio cartaceo possono accedere solo i diretti incaricati.

PERDITA DI DATI – SOGLIA DI RISCHIO BASSA – I dati sono conservati su dischi e sono effettuate periodicamente copie di backup.

INCAPACITA' DI RIPRISTINARE COPIE DI BACKUP – SOGLIA DI RISCHIO BASSA – I controlli periodici effettuati sui supporti di backup hanno sempre fornito esiti positivi.

CRITERI E MODALITA' PER IL SALVATAGGIO/RIPRISTINO DEI DATI PERSONALI

Nome della banca dati: ARGO BACKUP

Contenuto: DATI DEL PERSONALE DOCENTE ED ATA, DEI GENITORI, DEGLI STUDENTI,
DEI FORNITORI E DEGLI ESPERTI

ISTITUTO DI ISTRUZIONE SUPERIORE "PRIMO LEVI" – CODICE DELLA PRIVACY – Pag. 25

31/03/2006

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Titolare del **ISTITUTO DI ISTRUZIONE SUPERIORE "PRIMO LEVI"** **Art. 34 D.Lgs**
Trattamento: **DIRIGENTE SCOLASTICO PROF. LAMBERTO PILLONETTO** **n. 196/2003**

Responsabile delle copie di sicurezza: SIG. ROBERTO PIVA
ASSISTENTE AMMINISTRATIVO

Periodicità del backup: SETTIMANALE

Numero copie di backup: 1

Tipo di supporto del backup: DISCO FISSO RIMOVIBILE

Luogo di conservazione del backup: ARMADIO SITUATO NELL'UFFICIO AMMINISTRATIVO

Periodicità della verifica del backup: MENSILE

INFORMAZIONI DA RIPORTARE NEL SUPPORTO

L'etichetta del supporto deve contenere il nome della banca dati, la data e l'ora di effettuazione del backup.

MODALITA' OPERATIVE DI BACKUP

Le procedure di backup devono essere eseguite in un momento di non attività degli incaricati ovvero questi devono essere preventivamente avvertiti di fermare l'attività di trattamento. La banca dati verrà copiata in un supporto rimovibile. Al termine dell'operazione il supporto rimovibile sarà conservato in un luogo protetto e sicuro.

MODALITA' OPERATIVE DI VERIFICA

La verifica del backup è effettuata verificando la leggibilità del supporto e l'integrità dei file copiati su di esso. A discrezione dell'Incaricato potranno essere ripristinate delle copie in un elaboratore esplicitamente predisposto alla verifica del backup. Al termine della verifica le copie ripristinate dovranno essere distrutte a cura dell'incaricato.

MODALITA' OPERATIVE DI RIPRISTINO

Il ripristino della banca dati è effettuato con modalità inverse a quelle del backup.. La banca dati, all'interno del supporto rimovibile, sarà spostata nella sede di quella danneggiata che verrà soprascritta o preventivamente distrutta.

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Titolare del **ISTITUTO DI ISTRUZIONE SUPERIORE "PRIMO LEVI"** **Art. 34 D.Lgs**
Trattamento: **DIRIGENTE SCOLASTICO PROF. LAMBERTO PILLONETTO** **n. 196/2003**

7.4 ANALISI DEI RISCHI SULLE RISORSE SOFTWARE

Il livello di sicurezza dei dati contenuti nei Personal Computer è dettato dalla presenza di idonee password di accesso sia alla rete che ai vari programmi.

Ad ogni addetto viene assegnata una password per l'accesso in rete con scadenza automatica dopo 6 mesi.

La password è personalizzata e definita direttamente dai vari utenti.

In caso di smarrimento e/o assenza dell'addetto, il Titolare del trattamento o chi per esso precedentemente autorizzato, può accedere lo stesso mediante sovrascrizione della password stessa (sostituendola completamente).

Per quanto riguarda tutti gli altri programmi il consenso è definito dal Titolare del trattamento o chi per esso, precedentemente autorizzato. Anche questi accessi sono gestiti e personalizzati mediante ulteriori password.

I floppy disk contenenti file, che a loro volta contengano dati dei clienti, possono essere riutilizzati esclusivamente previa formattazione del floppy stesso, in modo da impedire la lettura dei dati precedenti. I floppy disk contenenti dati sono custoditi in appositi contenitori di plastica.

ELEMENTI DI RISCHIO E PRECAUZIONI ADOTTATE

ACCESSO NON AUTORIZZATO ALLE BASI DATI CONNESSE – SOGLIA DI RISCHIO BASSA – I software che trattano i dati controllano l'accesso tramite una finestra di autenticazione.

ERRORI SOFTWARE CHE MINACCIANO L'INTEGRITA' DEI DATI – SOGLIA DI RISCHIO BASSA – I software sono utilizzati da parecchi anni e non hanno mai causato la perdita o il danneggiamento dei dati trattati.

PRESENZA DI CODICE NON CONFORME ALLE SPECIFICHE DEL PROGRAMMA – SOGLIA DI RISCHIO BASSA – I programmi sono forniti da produttori che operano nel settore con la massima serietà da molti anni.

7.5 ANALISI DEI RISCHI SULL'ARCHIVIAZIONE DI TIPO CARTACEO

Negli Uffici sono presenti dei luoghi sicuri (armadi) ove sono custoditi gli archivi cartacei.

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Titolare del **ISTITUTO DI ISTRUZIONE SUPERIORE "PRIMO LEVI"** **Art. 34 D.Lgs**
Trattamento: **DIRIGENTE SCOLASTICO PROF. LAMBERTO PILLONETTO** **n. 196/2003**

L'accesso al locale avviene tramite una porta protetta da serratura.

Dal luogo sicuro sono asportati solo i documenti strettamente necessari per le operazioni di trattamento. Al termine delle operazioni di trattamento, i documenti sono immediatamente riposti nel luogo sicuro.

Per tutto il periodo in cui i documenti sono all'esterno del luogo sicuro, l'incaricato non li perde mai di vista, adempiendo ad un preciso obbligo di custodia dei documenti stessi.

L'incaricato inoltre controlla che i documenti, composti da numerose pagine o più raccoglitori, siano sempre completi, verificando sia il numero di fogli che l'integrità del contenuto, rispetto a quanto presente all'atto del prelievo dal luogo sicuro.

Se, per qualche motivo si devono abbandonare in ufficio i documenti, l'incaricato identifica un luogo sicuro di custodia temporanea, che dia sufficienti garanzie di protezione da accessi non autorizzati (cassettera o armadio con chiusura a chiave).

I documenti di cui sopra non saranno mai lasciati incustoditi sul tavolo durante il giorno.

Si adottano tutte le misure preventive nel caso in cui un visitatore o terzo (addetti alla manutenzione, alle pulizie, o colleghi non autorizzati) possa entrare in ufficio anche non invitato o per cause accidentali e possa venire a conoscenza dei contenuti dei documenti.

Tali misure consistono nel rovesciare sotto-sopra i primi fogli presenti sul tavolo oppure coprirli mediante cartelline e/o altri mezzi atti a evitare letture indiscrete.

Le eventuali rubriche telefoniche in utilizzo su supporto cartaceo sono richiuse dopo la consultazione ed il primo foglio delle rubriche stesse, leggibile all'esterno, non contiene alcun dato di cliente.

Le copie dei telefax inviati mediante apparecchio tradizionale sono riconsegnate a colui che eseguito o fatto eseguire la trasmissione, avendo cura di porre quale primo foglio il rapporto di trasmissione formato A4 che viene stampato dal fax, con di seguito i fogli contenenti il messaggio.

Per ciò che concerne la trasmissione del telefax, è stata inserita nella copertina del messaggio la seguente dicitura:

"Le informazioni contenute nella presente comunicazione ed i relativi allegati possono essere riservate e sono, comunque, destinate esclusivamente alle persone o alla Società indicate quali destinatari. La diffusione, distribuzione, e/o copiatura del documento trasmesso da parte di qualsiasi soggetto diverso dal destinatario è proibita, sia ai sensi dell'art. 616 c.p. , che ai sensi del D.Lgs. n. 196/2003.

Se avete ricevuto questo messaggio per errore, vi preghiamo di distruggerlo e di informarci immediatamente per telefono allo **0423/23523** o inviando un messaggio all'indirizzo e-mail.: segreteria@liceolevi.it".

ELEMENTI DI RISCHIO E PRECAUZIONI ADOTTATE

PERDITA DI DATI – SOGLIA DI RISCHIO MEDIA – Nei locali tutti gli armadi sono dotati di serratura.

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Titolare del **ISTITUTO DI ISTRUZIONE SUPERIORE "PRIMO LEVI"** **Art. 34 D.Lgs**
Trattamento: **DIRIGENTE SCOLASTICO PROF. LAMBERTO PILLONETTO** **n. 196/2003**

8 MISURE DI CONTROLLO DEI RISCHI

In ottemperanza agli artt. 31, 32, 33, 34, 35 e 36 del D.Lgs. 30/06/2003 n. 196, il presente DPS prevede l'organizzazione di idonee misure di sicurezza da adottare, volte a garantire la sicurezza dei dati. La sicurezza dei dati si esplica nella loro diligente custodia, al fine di prevenirne alterazioni, distruzione, diffusioni non autorizzate o trattamenti non conformi alle finalità della raccolta.

I Responsabili della sicurezza e del trattamento o, in mancanza, il Titolare, appronteranno tutti i mezzi necessari per il perseguimento dei fini legati alla sicurezza dei dati, sfruttando anche le conoscenze acquisite in base al progresso tecnico.

Sono previste specifiche misure di sicurezza, sia per quanto riguarda la custodia di archivi elettronici e non, che l'accesso ai locali ove i dati oggetto del trattamento sono fisicamente conservati.

La procedura di preservazione dal rischio di perdita dei dati trattati con mezzi informatici, o dalla divulgazione autorizzata, si esplica nella previsione di un piano basato su:

1 Copie periodiche di Backup. Tale procedura, che il Responsabile della sicurezza o il Titolare stileranno di concerto con il Responsabile della gestione e manutenzione degli elaboratori elettronici, dovrà fornire le istruzioni e le modalità in merito al tipo di supporto utilizzato, all'impiego di specifici software per salvataggi automatizzati, alla nomina degli Incaricati delle copie di sicurezza delle banche dati, alla custodia dei supporti nei quali sono stati memorizzati i dati, alla distruzione dei supporti dopo un certo periodo o in ogni modo alla cancellazione dei dati dai supporti di Backup in maniera tale da impedire ogni possibile consultazione.

La procedura di salvataggio prevede anche il monitoraggio di tutte le operazioni affinché il Responsabile o il Titolare possano individuare periodicamente circostanze che impongano l'adozione di un diverso piano di Backup o il suo aggiornamento.

Il salvataggio dei dati dovrà avvenire con cadenza almeno settimanale.

2 Protezione da virus informatici o intrusioni non autorizzate nella propria rete informatica. Il Responsabile della sicurezza o il Titolare incaricano il Responsabile della gestione e manutenzione degli elaboratori elettronici ad approntare tutte le misure di sicurezza idonee a prevenire e ridurre infezioni da virus informatici o da intrusioni non autorizzate nel sistema.

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Titolare del **ISTITUTO DI ISTRUZIONE SUPERIORE "PRIMO LEVI"** **Art. 34 D.Lgs**
Trattamento: **DIRIGENTE SCOLASTICO PROF. LAMBERTO PILLONETTO** **n. 196/2003**

Il Responsabile provvederà a dettagliare tutte le misure adottate compresi l'utilizzo di appositi programmi Antivirus, Firewall e di qualsiasi ulteriore soluzione informatica che ritenesse opportuna per diminuire la vulnerabilità del sistema.

E' anche compito del Responsabile pianificare il lavoro relativo all'installazione degli aggiornamenti messi a disposizione dalle case produttrici di software per correggere i difetti dei programmi o dei sistemi operativi utilizzati. Il Responsabile può prevedere anche che il periodico aggiornamento dei programmi utilizzati per garantire la sicurezza informatica avvenga in un arco di tempo inferiore a quanto previsto dal D.Lgs. 30/06/2003 n. 196, annuale o semestrale nel caso di dati sensibili o giudiziari.

Tutte le misure di sicurezza previste dal Responsabile della gestione e manutenzione degli elaboratori elettronici dovranno essere periodicamente valutate per adattare la procedura all'evoluzione tecnologica.

Il Responsabile della gestione e manutenzione degli elaboratori elettronici dovrà provvedere ed istruire adeguatamente eventuali Incaricati al trattamento.

In caso di infezione del sistema da parte di virus informatici, il Responsabile della gestione e manutenzione degli elaboratori elettronici dovrà tempestivamente adottare tutte le misure idonee per isolare il sistema ed evitare che il danno venga esteso ad altri elaboratori; dovrà quindi individuare le cause di tale infezione e provvedere a rimuoverle.

3 Sistema di autenticazione informatica. Così come previsto dall'Allegato B al D.Lgs. n.196/2003, il trattamento dei dati personali con strumenti elettronici è consentito solo agli incaricati dotati di credenziali di autenticazione che consentono il superamento di una procedura di autenticazione. Il Responsabile del trattamento (o, in mancanza, il Titolare), in accordo con il Responsabile della gestione e manutenzione degli elaboratori elettronici, definisce le modalità di assegnazione delle credenziali di autenticazione agli Incaricati del trattamento. Le credenziali possono consistere nell'assegnazione di User ID e password o nell'utilizzo di dispositivi associati ad un codice identificativo o anche ad una caratteristica biometrica. Ad ogni soggetto autorizzato all'accesso alle banche dati possono essere assegnate anche più credenziali per l'autenticazione in base alle esigenze organizzative o al numero di banche dati gestite.

Se fra le credenziali è prevista l'assegnazione di una password, questa non deve essere di lunghezza inferiore agli otto caratteri (o al numero massimo possibile se lo strumento elettronico utilizzato non lo consente); non deve contenere nomi comuni, nomi di persona o riferimenti agevolmente riconducibili all'incaricato, e, in quanto personale, non deve essere trascritta. Al primo utilizzo delle password, l'incaricato provvederà a modificarla e, successivamente, la modificherà periodicamente con cadenza almeno semestrale, a meno che la banca dati non contenga dati sensibili; in tal caso la parola chiave andrà modificata ogni tre mesi.

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Titolare del **ISTITUTO DI ISTRUZIONE SUPERIORE "PRIMO LEVI"** **Art. 34 D.Lgs**
Trattamento: **DIRIGENTE SCOLASTICO PROF. LAMBERTO PILLONETTO** **n. 196/2003**

Ogni persona incaricata al trattamento dei dati deve adottare tutte le cautele possibili per garantire la segretezza delle credenziali di autenticazione assegnate.

Per ciò che concerne la gestione dei dati non trattati con strumenti elettronici, viene appositamente definita la modalità di trattamento ed i vari supporti utilizzati. Vengono altresì definite tutte le misure di sicurezza da adottare per evitare l'accidentale perdita o danneggiamento dei dati.

Per garantire la protezione dei dati, inoltre, sarà assegnato un ruolo di responsabilità alla figura che si occuperà della pulizia degli uffici aziendali e dei luoghi in cui sono custoditi i dati personali.

Il suddetto responsabile si impegnerà ad adottare tutte le misure necessarie per garantire la sicurezza dei dati tenendo un comportamento lecito e corretto. Inoltre, sarà messo a conoscenza del contenuto del Documento Programmatico sulla sicurezza.

In ogni caso è fatto divieto a qualunque soggetto di divulgare informazioni concernenti i dati oggetto del trattamento, effettuarne copie di qualsiasi natura (su supporti cartacei, informatici, audiovisivi ecc.) e distruggere, sottrarre o manipolare il contenuto della banche dati se non espressamente autorizzato dal Responsabile o dal Titolare.

Per diminuire il rischio, cioè' la probabilità di accadimento e l'impatto di un evento dannoso, sono disponibili quattro tipi di contromisure:

1 L'ELIMINAZIONE

2 LA PREVENZIONE

3 IL CONTENIMENTO

4 IL TRASFERIMENTO

L' ELIMINAZIONE DEL RISCHIO rappresenta l'intervento più radicale, ma non proponibile in forma sistematica. Il criterio di eliminazione sarà preso in considerazione nell'ipotesi che non sia ragionevolmente possibile allestire una difesa del sito, congrua con la temibilità dell'evento, provvedendo quindi al suo spostamento.

LA PREVENZIONE è la più attraente misura di difesa e di sicurezza perché consente di diminuire la probabilità che si manifesti un danno. Essa si basa sull'adozione di misure di protezione, che scoraggiano l'intruso (impianti antintrusione), che bloccano il vandalo (vetri antisfondamento), che impediscono l'innescare di incendi (uso di materiale ignifugo) e che impediscono infortuni.

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Titolare del **ISTITUTO DI ISTRUZIONE SUPERIORE "PRIMO LEVI"** **Art. 34 D.Lgs**
Trattamento: **DIRIGENTE SCOLASTICO PROF. LAMBERTO PILLONETTO** **n. 196/2003**

Le misure di CONTENIMENTO DEL RISCHIO mirano a limitare gli effetti dannosi provocati dall'accadimento dell'evento temuto. Spesso la natura dei luoghi e degli oggetti protetti rende difficile l'adozione di appropriate misure di prevenzione del rischio oppure, quale che sia il livello di prevenzione attuato, è impossibile affermare che l'evento dannoso non possa verificarsi. Un classico esempio di tale tipo di misura, sia in materia di protezione dall'incendio che dal furto, è la compartimentazione dei locali.

La più classica forma di TRASFERIMENTO DEL RISCHIO è la copertura assicurativa. Tale forma di difesa è popolarissima ed efficace per tutti i rischi che producano conseguenze di natura esclusivamente patrimoniale e monetizzabile.

8.1 MISURE DI SICUREZZA FISICHE

Le misure di sicurezza FISICHE hanno la proprietà di essere le uniche che effettivamente impediscono o rallentano l'attacco in corso.

Presso l'attività oggetto di tale valutazione sono presenti le seguenti misure di sicurezza fisiche:

SERVER

IMPIANTI DI LUCE DI EMERGENZA

ARMADI CON SERRATURA

ANALISI DELLA MISURE ADOTTATE

CUSTODIA DEGLI ARCHIVI CARTACEI IN ARMADI CHIUSI A CHIAVE :

Tutti i documenti cartacei contenenti dati personali sono conservati nel locale adibito ad archivio in armadi dotati di serratura. Gli incaricati possono prelevare i documenti necessari per il trattamento per il tempo necessario a tale operazione e quindi devono riporli nel sopraccitato luogo preposto alla loro conservazione.

CUSTODIA DEI SUPPORTI MAGNETICI:

I supporti magnetici utilizzati per l'attività di backup sono conservati in un luogo sicuro all'interno dei locali.

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Titolare del **ISTITUTO DI ISTRUZIONE SUPERIORE "PRIMO LEVI"** **Art. 34 D.Lgs**
Trattamento: **DIRIGENTE SCOLASTICO PROF. LAMBERTO PILLONETTO** **n. 196/2003**

DISPOSITIVI ANTINCENDIO

I locali della sede sono dotati di estintori per la soppressione di focolai di incendio.

CONTINUITA' DELL'ALIMENTAZIONE ELETTRICA

I Personal Computer sono collegati ad un server che garantisce una stabilizzazione dell'energia elettrica erogata. Tale gruppo, in conseguenza di un'improvvisa assenza di energia, garantisce un'autonomia temporale necessaria ad avviare le corrette procedure di spegnimento dell'elaboratore

8.2 MISURE DI SICUREZZA LOGICHE

Le misure di sicurezza LOGICHE non possono impedire l'accesso agli estranei, ma sono in grado di segnalare l'intrusione in atto.

ANALISI DELLA MISURE ADOTTATE

IDENTIFICAZIONE DEGLI INCARICATI PREPOSTI ALLE ATTIVITA' DI TRATTAMENTO

Sono stati individuati e nominati per iscritto gli incaricati preposti al trattamento. Agli incaricati, congiuntamente alla lettera di nomina, sono state indicate le norme operative e di sicurezza a cui attenersi.

ASSEGNAZIONE ED AUTORIZZAZIONE DEGLI ELABORATORI SU CUI EFFETTUARE I TRATTAMENTI

Ad ogni incaricato è stato assegnato un elaboratore tramite il quale potrà accedere agli archivi in formato elettronico su cui operare i trattamenti.

INDICAZIONE DEI CODICI IDENTIFICATIVI E DELLE PAROLE CHIAVE AGLI INCARICATI

Gli incaricati sono stati contraddistinti da codici identificativi univoci (USER ID) che neppure in futuro potranno essere associati ad altre persone.

Le parole chiave assegnate inizialmente dal custode delle password sono state cambiate al primo accesso dagli incaricati.

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Titolare del **ISTITUTO DI ISTRUZIONE SUPERIORE "PRIMO LEVI"** **Art. 34 D.Lgs**
Trattamento: **DIRIGENTE SCOLASTICO PROF. LAMBERTO PILLONETTO** **n. 196/2003**

Le nuove parole chiave impostate dagli incaricati sono state consegnate in una busta sigillata al custode delle password. Quest'ultima procedura sarà effettuata ogni qualvolta un incaricato cambierà autonomamente una delle proprie password.

INDICAZIONE DEL CUSTODE DELLE PASSWORD

E' stato individuato e nominato per iscritto il custode delle password a cui spetta la custodia, in un luogo sicuro, delle password a lui affidate dagli incaricati.

PREDISPOSIZIONE ED AGGIORNAMENTO DEGLI ANTIVIRUS

Gli elaboratori sono protetti con programmi antivirus.

INDICAZIONE DELL'AMMINISTRATORE DI SISTEMA

E' stato individuato e nominato per iscritto l'amministratore di sistema cui è stato affidato il compito di sovrintendere alle risorse dei sistemi operativi degli elaboratori e delle basi dati; sarà compito dell'amministratore, su indicazione del titolare del trattamento, disattivare i codici identificativi in caso di mancato utilizzo per un periodo superiore ai sei mesi.

8.3 MISURE DI SICUREZZA PROCEDURALE

Le misure di sicurezza PROCEDURALE hanno il compito di garantire la corretta funzionalità delle misure descritte in precedenza e di assicurare in tempi brevi gli interventi del caso. Vi sono procedure che gestiscono l'attivazione delle difese, procedure che gestiscono il loro ripristino in caso di anomalia funzionale (procedure di manutenzione) e procedure che garantiscono l'intervento ed il blocco dell'intruso.

ANALISI DELLE MISURE ADOTTATE

ANALISI DEI RISCHI E DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Sulla base dell'analisi dei rischi è stato redatto il presente documento programmatico sulla sicurezza. Questo documento sarà divulgato a tutte le funzioni aziendali.

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Titolare del **ISTITUTO DI ISTRUZIONE SUPERIORE "PRIMO LEVI"** **Art. 34 D.Lgs**
Trattamento: **DIRIGENTE SCOLASTICO PROF. LAMBERTO PILLONETTO** **n. 196/2003**

PIANO DI VERIFICA DELLE MISURE ADOTTATE

E' stato stabilito un piano di verifica della misure adottate. Tale piano è illustrato nel presente Documento Programmatico sulla Sicurezza.

PIANO DI FORMAZIONE DEGLI INCARICATI

E' stato predisposto un piano di formazione degli incaricati. Tale piano è illustrato nel presente Documento Programmatico sulla Sicurezza.

DOTAZIONE DI DISPOSITIVI ANTINTRUSIONE

L'entrata principale dell'Istituto, l'ingresso lato nord e l'accesso alla palestra sono protetti da saracinesche.

CUSTODIA DI DOCUMENTI CARTACEI

Tutti i documenti cartacei contenenti dati personali, tranne per i periodi strettamente necessari alle operazioni di trattamento, sono custoditi in armadi dotati di serratura.

9 PIANO DI AUTOCONTROLLO ADOTTATO

Periodicamente e comunque ad ogni revisione del Documento Programmatico sulla Sicurezza il Titolare del trattamento dei dati personali effettua le seguenti operazioni per mantenere i livelli di rischio al minimo di legge:

- 1 Verifica del funzionamento dell'impianto di emergenza;
- 2 Manutenzioni periodiche (frequenza semestrale) dei mezzi di estinzione portatile e dell'impianto fisso antincendio;
- 3 Verifica e manutenzione dei gruppi di continuità;
- 4 Verifica del corretto utilizzo della parole chiave e dei profili di accesso degli incaricati;
- 5 Verifica degli aggiornamenti dei programmi antivirus;
- 6 Verifica delle procedure di backup;

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Titolare del **ISTITUTO DI ISTRUZIONE SUPERIORE "PRIMO LEVI"** **Art. 34 D.Lgs**
Trattamento: **DIRIGENTE SCOLASTICO PROF. LAMBERTO PILLONETTO** **n. 196/2003**

- 7 Verifica della efficacia del metodo di conservazione dei documenti cartacei;
- 8 Accertamento della distruzione dei supporti magnetici che non possono più essere riutilizzati;
- 9 Verifica del livello di formazione degli incaricati.

10 CRITERI DI RIPRISTINO DATI DANNEGGIATI

In caso di distruzione o danneggiamento dei dati oggetto del trattamento, l'Incaricato delle copie di sicurezza delle banche dati, di concerto con il Responsabile della gestione e manutenzione degli strumenti elettronici, provvederà a ripristinare i dati mediante utilizzo delle copie di backup.

L'Incaricato può anche prevedere l'utilizzo di altri strumenti in suo possesso (supporti cartacei, e-mail, registrazioni audiovisive ecc.) per ricostruire nel modo più fedele possibile i dati distrutti o danneggiati, sia quelli trattati con l'ausilio di strumenti elettronici che quelli trattati con altri tipi di strumenti. In caso di distruzione o danneggiamento degli strumenti utilizzati per l'accesso ai dati, il Responsabile della gestione e manutenzione degli elaboratori elettronici (o in mancanza un incaricato nominato dal Responsabile o dal Titolare) provvederà tempestivamente al ripristino del normale stato di utilizzo dei suddetti strumenti o alla loro sostituzione.

La procedura di ripristino o di accesso ai dati avverrà comunque in tempi compatibili con i diritti degli interessati in conformità al punto 23 dell'allegato B del D.Lgs. 196/2003, il quale prevede un periodo di tempo non superiore a sette giorni.

Ad ogni evento che comporti distruzione, danneggiamento o problemi di accesso ai dati dovrà essere opportunamente aggiornata l'analisi dei rischi di cui al punto 4 del presente Documento Programmatico sulla Sicurezza.

11 PIANO DI FORMAZIONE DEGLI INCARICATI

Al Responsabile della sicurezza (o in mancanza al Titolare) spetta il compito di provvedere all'opportuna formazione di tutti gli incaricati al trattamento dei dati al fine di:

- 1 Garantire il massimo rispetto della procedure elencate nel presente Documento Programmatico sulla Sicurezza;
- 2 Rendere edotto il personale dei rischi che incombono sui dati;
- 3 Informare il personale sulle responsabilità che ne derivano.

Il Responsabile della sicurezza (o in mancanza il Titolare) valuterà opportunamente il livello di preparazione dei singoli addetti in merito alle procedure (informatiche e non) utilizzate per il trattamento e la custodia dei dati.

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Titolare del **ISTITUTO DI ISTRUZIONE SUPERIORE "PRIMO LEVI"** **Art. 34 D.Lgs**
Trattamento: **DIRIGENTE SCOLASTICO PROF. LAMBERTO PILLONETTO** **n. 196/2003**

Eventuali lacune saranno colmate con appositi interventi formativi volti a rendere i soggetti interessati idonei a svolgere gli incarichi loro assegnati.

Il Titolare o il Responsabile, con cadenza almeno annuale, provvederanno a verificare le esigenze di formazione del personale in base all'esperienza acquisita, al progresso tecnologico o al cambiamento di mansioni.

12 DATI AFFIDATI ALL'ESTERNO DELLA STRUTTURA

Qualora il trattamento dei dati venisse affidato in parte o in toto a soggetti esterni alla struttura, la nomina di tali soggetti avverrà per iscritto mediante apposita lettera di incarico.

Sarà cura del Titolare conservare in luogo sicuro copia di tale lettera.

Sarà compito del soggetto esterno (Titolare) nominare un eventuale Responsabile e comunque nominare gli incaricati ed impartire loro la dovuta istruzione per garantire il trattamento e la conservazione dei dati in modo puntuale, lecito e sicuro in base ai criteri previsti dal D.Lgs. n. 196/2003.

13 CIFRATURA DEI DATI RELATIVI ALLO STATO DI SALUTE

Qualora la tipologia dei dati trattati comprendesse anche quelli di tipo sanitario relativi allo stato di salute o alla vita sessuale verranno previste idonee misure per gestire la separazione dei dati dall'individuazione diretta dell'interessato e per identificare i casi in cui necessita la loro cifratura.

ANALISI DEGLI ELEMENTI DI RISCHIO E DELLA MSURE ADOTTATE

ACCESSO AI LOCALI – PORTE CON CHIUSURA

PROTEZIONE DELLE PORTE DI ACCESSO – TUTTE LE PORTE DI ACCESSO SONO DOTATE DI SERRATURA

PROTEZIONE DEGLI ARCHIVI CARTACEI – E' PRESENTE UN SISTEMA DI CHIUSURA CON SERRATURA

MISURE ANTINCENDIO – SONO PRESENTI ESTINTORI

SOFTWARE – TUTTI I SOFTWARE SONO CERTIFICATI

ISTITUTO DI ISTRUZIONE SUPERIORE "PRIMO LEVI" – CODICE DELLA PRIVACY – Pag. 37

31/03/2006

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Titolare del **ISTITUTO DI ISTRUZIONE SUPERIORE "PRIMO LEVI"** **Art. 34 D.Lgs**
Trattamento: **DIRIGENTE SCOLASTICO PROF. LAMBERTO PILLONETTO** **n. 196/2003**

PASSWORD – TUTTI I PERSONALE COMPUTER SONO MUNITI DI PASSWORD DI ACCESSO

BACKUP – PERIODICAMENTE VIENE EFFETTUATO IL BACKUP

ANTISPAMMING – FORNITI DAL SISTEMA OPERATIVO IN OGNI PERSONALE COMPUTER

FIREWALL – FORNITI DAL SISTEMA OPERATIVO IN OGNI PERSONALE COMPUTER

SERVER – TUTTI I PERSONAL COMPUTER SONO COLLEGATI AD UN SERVER

ANTIVIRUS – TUTTI I PERSONALE COMPUTER SONO PROVVISI DI SOFTWARE ANTIVIRUS

14 REVISIONE DEL DOCUMENTO

Il presente Documento Programmatico sulla Sicurezza deve essere revisionato entro il

31 MARZO 2007

IL TITOLARE DEL TRATTAMENTO
(PROF. LAMBERTO PILLONETTO)