ISTITUTO TECNICO COMMERCIALE E PER GEOMETRI
" V. PARETO"
Via Annecchino, 252 – 80078 Pozzuoli (NA)
Tel.: 081/8664962; **Fax**: 081/5046777
C. M.: NATD130003; **e–mail**: natd130003@istruzione.it

6.4.1.6 Censimento dei fax

Codice identificativo	Ubicazione (Codice area)	Descrizione
Fax1	P1.1	Canon L800

6.5 STRUTTURA ORGANIZZATIVA FUNZIONALE AL TRATTAMENTO DATI E SINGOLE RESPONSABILITÀ

6.5.1 Struttura organizzativa-funzionale

FUNZIONE	RESPONSABILE
Titolare del trattamento	Dirigente Scolastico
Responsabile del trattamento	DSGA
Custode delle password	DSGA (ARGO, Server), DS (Scuolanet)
Amministratore di Sistema	DSGA (ARGO), AT (account Server e client), DS (Scuolanet x docenti)
Incaricati del trattamento	Collaboratori del Dirigente Scolastico, Docenti, AA, AT, CS, DSGA

L'elenco nominativo degli incaricati a qualsiasi titolo è tenuto dal Titolare del trattamento o dal Responsabile del Trattamento in luogo sicuro, modificato da questi ad ogni variazione organizzativa e messo a disposizione degli interessati che ne facciano specifica richiesta.

6.5.2 Responsabilità

6.5.2.1 Il Titolare del trattamento

È onere del Titolare del trattamento dei dati personali, ove lo ritenga necessario, individuare, nominare e incaricare per iscritto uno o più Responsabili del trattamento dei dati che assicurano e garantiscono che vengano adottate le misure di sicurezza ai sensi dell'art. 29 del D. Lgs 196/03. Il Titolare del trattamento affida al Responsabile del trattamento dei dati il compito di adottare le misure tese a ridurre al minimo il rischio di distruzione dei dati, l'accesso non autorizzato o il trattamento non consentito, previe idonee istruzioni fornite per iscritto. Inoltre, il Titolare nomina anche il Custode delle password e l'Amministratore del sistema.

Il Titolare del trattamento deve consegnare a ciascun Responsabile del trattamento, al Custode delle password e all'Amministratore del sistema una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina e li deve informare delle rispettive responsabilità che sono loro affidate in relazione a quanto disposto dalle normative in vigore ed, in particolare, di quanto stabilito dal D. Lgs 196/03.

Ove il Responsabile del trattamento dei dati non è nominato, il Titolare del trattamento assume direttamente le responsabilità di cui al paragrafo dal titolo "Il Responsabile del trattamento". Anche nel caso che il Titolare assuma direttamente le funzioni di Custode delle password e Amministratore del sistema, i relativi compiti di cui ai paragrafi inerenti sono da egli assunti.

In caso di assenza di un incaricato e vista l'urgenza di trattare dati cui solo questi può accedere, il Titolare impartisce istruzioni scritte al Custode delle password e al Responsabile (se nominati) circa l'apertura della busta contenente i codici di autenticazione e, quindi, provvedere con altro incaricato.

Il titolare del trattamento gestisce in prima persona l'assegnazione delle user id e della 1a password per gli alunni e i loro genitori e per i docenti del sistema "Scuolanet" per la gestione dei dati personali riguardanti le valutazioni degli alunni e le loro assenze. Il titolare del trattamento fa anche da custode delle password per i docenti per tale sistema.

6.5.2.2 Il Responsabile del trattamento

Il Responsabile del Trattamento ha l'onere d'individuare, nominare e indicare per iscritto gli incaricati del trattamento. Inoltre, il Responsabile ha il compito di:

1. redigere e aggiornare ad ogni variazione l'elenco dei sistemi di elaborazione;
2. redigere e aggiornare l'elenco delle tipologie dei trattamenti effettuati;
3. attribuire, con l'ausilio dell'Amministratore di sistema, ad ogni incaricato un codice identificativo (user id) per l'utilizzazione dell'elaboratore che deve essere individuale e non riutilizzabile;
4. autorizzare i singoli incaricati ad uno specifico trattamento o ad un insieme di trattamenti;
5. verificare, con l'ausilio dell'amministratore del sistema, con cadenza almeno quadrimestrale, l'efficacia dei programmi di protezione e antivirus;
6. definire le modalità di accesso ai locali e le misure indicate al paragrafo dal titolo "Misure di sicurezza contro il rischio di accesso non autorizzato";
7. garantire che tutte le misure di sicurezza riguardanti i dati in possesso dell'Istituzione Scolastica siano applicati;
8. informare il Titolare dell'eventualità che siano rilevate nuove tipologie di rischio;
9. prendere tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvedere al ricovero periodico degli stessi con copie di back-up;
10. assicurarsi della qualità delle copie di back-up dei dati e della loro conservazione in luogo adatto e sicuro.

La nomina del Responsabile del trattamento deve essere effettuata con lettera d'incarico, deve essere controfirmata dall'interessato per accettazione e copia della lettera di nomina accettata deve essere conservata a cura del Titolare in luogo sicuro. La nomina è a tempo indeterminato, può essere revocata in qualsiasi momento dal Titolare senza preavviso ed, eventualmente, affidata ad altro soggetto.

6.5.2.3 Il Custode delle password

Il Custode delle password ha il compito di custodire le buste sigillate contenenti le parole chiavi o password per l'accesso ai dati archiviati nei sistemi di elaborazione dati.

Il Custode delle password deve predisporre, per ogni incaricato del trattamento, una busta chiusa e siglata sulla quale è indicato il nominativo; all'interno della busta deve essere indicato, a cura dell'incaricato, la user-id e la password per accedere alle banche dati. Il Custode delle password provvede a conservare tali buste in luogo chiuso e protetto. Il Custode delle password deve revocare, su comunicazione dell'Amministratore del sistema, tutte le password non utilizzate per un periodo superiore a 6 mesi. Periodicamente, rileva le buste vecchie di 3 mesi e lo comunica all'utente che dovrà provvedere alla sostituzione della password.

La nomina del Custode delle password deve essere effettuata con lettera d'incarico, deve essere controfirmata dall'interessato per accettazione e copia della lettera di nomina accettata deve essere conservata a cura del Titolare in luogo sicuro. La nomina è a tempo indeterminato, può essere revocata in qualsiasi momento dal Titolare senza preavviso ed, eventualmente, affidata ad altro soggetto.

6.5.2.4 L'Amministratore del sistema

Il Titolare specifica all'Amministratore del sistema le reti, gli elaboratori e le banche dati che è chiamato a sovrintendere. È compito dell'Amministratore di sistema:

1. fare in modo che sia prevista la disattivazione dei codici identificativi personali (user-id) in caso di perdita della qualità che consentiva all'incaricato l'accesso all'elaboratore, oppure nel caso di mancato utilizzo dei codici identificativi personali per oltre 6 mesi;
2. proteggere gli elaboratori dal rischio d'intrusione (violazione del sistema da parte di "hacker" o "cracker") e dal rischio di virus mediante idonei programmi;
3. deve istruire gli incaricati per distruggere o cancellare i supporti magnetici utilizzati per memorizzare dati personali;
4. per i sistemi informatici che ospitano banche dati, obbligo di password di BIOS da comunicare all'incaricato responsabile di sistema.
5. effettuare, controllare e conservare in luogo sicuro le copie di back up;
6. adempiere alle mansioni di custode delle password se non altrimenti stabilito.

In ottemperanza a quanto previsto dal Provvedimento del Garante del 27/11/2008 e pubblicato sulla G.U. n° 300 del 24/12/2008 si attuano tutte le disposizioni ivi previste.

La nomina dell'Amministratore del sistema deve essere effettuata con lettera d'incarico, deve essere controfirmata dall'interessato per accettazione e copia della lettera di nomina accettata deve essere conservata a cura del Titolare in luogo sicuro. La nomina è a tempo indeterminato, può essere revocata in qualsiasi momento dal Titolare senza preavviso ed, eventualmente, affidata ad altro soggetto.

6.5.2.5 Gli Incaricati del trattamento

La nomina, da parte del Responsabile del trattamento, di ciascun Incaricato del trattamento dei dati deve essere effettuata con lettera d'incarico in cui sono specificati i compiti affidati (profilo di autorizzazione).

Gli Incaricati del trattamento devono ricevere idonee istruzioni scritte (anche per gruppi omogenei di lavoro) sulle mansioni loro affidate e sugli adempimenti cui sono tenuti.

Agli Incaricati il Responsabile deve consegnare una copia di tutte le norme che riguardano la sicurezza del trattamento dati in vigore al momento della nomina. Agli Incaricati deve essere consegnato un codice identificativo personale. Gli Incaricati, correttamente istruiti sulla formulazione delle password, redigono un documento in cui associano alla propria user-id la relativa password personale e lo consegnano in busta chiusa, riportante all'esterno il proprio nominativo, al Custode delle password.

Le nomine sono effettuate anche per il **personale supplente temporaneo, docente e ATA,** e, per quanto riguarda i trattamenti effettuati con strumenti elettronici, per eventuale **personale esterno incaricato della manutenzione**.

La nomina degli Incaricati del trattamento dei dati deve essere controfirmata dall'interessato per presa visione e copia della stessa deve essere conservata a cura del Responsabile in luogo sicuro. La nomina degli Incaricati è a tempo indeterminato, può essere revocata in qualsiasi momento dal responsabile, per giustificato motivo, senza preavviso ed affidata ad altro soggetto; viene revocata con il venir meno dei compiti che giustificavano il trattamento dei dati personali.

6.6 DATI AFFIDATI AD ENTI ESTERNI PER IL TRATTAMENTO IN OUTSOURCING

Il Titolare può decidere di affidare il trattamento in tutto o in parte a soggetti terzi, in **out-sourcing**, nominandoli Responsabili del trattamento. In questo caso debbono essere specificati i soggetti interessati e i luoghi dove fisicamente avviene il trattamento dei dati stessi.

Nel caso in cui questi non vengono espressamente nominati, i Responsabili del trattamento in out-sourcing, ai sensi dell'art. 8 della Legge 675/96, devono intendersi autonomi titolari del trattamento e quindi soggetti ai corrispettivi obblighi e, pertanto, rispondono direttamente ed in via esclusiva per le eventuali violazioni alla legge.

Il Titolare deve informare il responsabile del trattamento dei dati in out-sourcing dei compiti che gli sono affidati in relazione a quanto disposto dalle normative in vigore ed, in particolare, di quanto stabilito dal D. Lgs 196/03.

Il Titolare o il Responsabile del trattamento, cui è affidato tale specifico incarico, deve redigere e aggiornare ad ogni variazione l'elenco dei soggetti che effettuano il trattamento dei dati in qualità di Responsabili del trattamento, con particolare attenzione a quei soggetti terzi in out-sourcing, ed indicare per ognuno di essi il tipo di trattamento effettuato.

Per l'inventario dei soggetti terzi in out-sourcing deve essere utilizzato un apposito modulo che deve essere conservato a cura del Responsabile in luogo sicuro.

Il Responsabile del trattamento dei dati in out-sourcing deve rilasciare una dichiarazione scritta al Titolare da cui risulti che sono state adottate le misure idonee di sicurezza per il trattamento dei dati secondo quanto disposto dal D. Lgs 196/03.

La nomina del responsabile in out-sourcing deve essere controfirmata per accettazione e copia della lettera di nomina accettata deve essere conservata a cura del titolare in luogo sicuro.

Attualmente l'Istituzione Scolastica affida all'esterno solo la manutenzione straordinaria dei sistemi informatici e applica, quindi, in questo caso, quanto previsto dal Provvedimento del Garante del 27/11/2008 circa la figura dell'Amministratore del Sistema.

6.7 IMPIANTO DI VIDEOSORVEGLIANZA

Non esiste impianto di video sorveglianza.

Per determinare i rischi occorre:

1. individuare le possibili minacce che possono essere condotte contro un sistema;
2. individuare i punti critici dello stesso.

Dall'incrocio di queste due dimensioni si possono prevedere i rischi e, quindi, determinare le strategie e gli accorgimenti per ridurli al massimo.

Gli attacchi possono determinare o una perdita di dati o un accesso ad essi non autorizzato.

7.1 NOZIONI GENERALI

I requisiti generici di sicurezza delle reti presentano le seguenti caratteristiche interdipendenti:

a. **Disponibilità:** i dati sono accessibili e i servizi sono ripristinabili anche in caso di interruzioni dovute alla cessazione dell'alimentazione elettrica, a catastrofi naturali, eventi imprevisti o ad attacchi di pirateria informatica;
b. **Autenticazione:** conferme dell'identità dichiarata da un utente;
c. **Integrità:** conferma che i dati trasmessi, ricevuti o conservati sono completi e inalterati;
d. **Riservatezza:** protezione dei dati trasmessi o conservati per evitarne l'intercettazione e la lettura da parte di persone non autorizzate. La riservatezza è particolarmente necessaria per la trasmissione di dati sensibili ed è uno dei requisiti che garantiscono il rispetto della vita privata.

Gli attacchi possono essere portati dalle seguenti tipologie di persone:

- **Hacker:** è l'informatico di grande esperienza e competenza che ha una conoscenza profonda del funzionamento e della struttura dei sistemi informatici. In particolare, l'hacker entra nei sistemi informatici altrui per dimostrare la propria abilità tecnica;
- **Cracker:** si introduce nei sistemi con scopi distruttivi o di interesse personale;
- **Lamer:** è un hacker dilettante;
- **Script kiddy:** il ragazzino degli script, ovvero un super dilettante che con strumenti preconfezionati trovati in rete può fare parecchi danni.

Nella maggior parte dei casi, gli attacchi informatici vengono effettuati da script kiddies che sperimentano tool (strumenti, cioè programmi) di hacking (di disturbo o distruzione, fatti dagli hacker) recuperati in rete.

7.2 PRINCIPALI MINACCE

Le principali fonti di rischio, o minacce, sono:

1. **Intrusioni:** persone non autorizzate accedono nei locali in cui sono presenti banche dati o penetrano nei sistemi informatici e consultano o alterano o copiano dati o documenti. *Contromisure:* per i sistemi informatici sono i **firewall, i proxy server, il sistema di account e password;** per i luoghi fisici sono **porte con serrature, registri d'ingresso e cartellini di riconoscimento.**
2. **Intercettazione delle comunicazioni:** le comunicazioni elettroniche possono essere intercettate e i dati in esse contenuti copiati o modificati. I punti più vulnerabili e sensibili ad una intercettazione del traffico sono i punti di gestione e di concentrazione della rete come i *router*, le *gateway* e i *server di rete.*

Contromisure: per i sistemi informatici sono i **firewall, i proxy server, il sistema di account e password;** per i luoghi fisici è il **trasporto dei dati sensibili in contenitori con serratura.**

3. **Virus:** sono piccoli programmi che si replicano automaticamente e che possono causare danni di vario tipo. Esempi: *virus del Kernel* (distruggono il cuore del sistema operativo), *virus eseguibile* (possono essere software maligni, detti malware ossia malicious software, che modificano o distruggono i dati), *virus delle macro* (in Word o Excel di Microsoft), *virus del Boot Sector* (si attivano quando si accende il computer e si duplicano sui supporti di memoria), *Bombe logiche* (rimangono inerti fino al momento in cui vengono innescati da un determinato evento), *worms* (non infettano gli altri programmi ma si auto duplicano in copie che, riproducendosi a loro volta, finiscono per saturare il sistema), *Trojans* (spiano il contenuto del computer e lo trasmettono all'esterno in maniera invisibile; spesso permettono un controllo remoto), *key sniffing* (registra ogni singolo tasto battuto, comprese le password e le trasmette via Internet).
   Contromisure: programmi antivirus, copie di back-up.
4. **Spy ware:** è un software che minaccia la privacy tracciando un profilo sulla base delle navigazioni in Internet.
   Contromisure: programmi di ricerca degli spy ware, programmi antivirus, firewall, proxy server.
5. **Attacchi alle impostazioni delle password:** *Brute force* (un apposito programma prova tutte le possibili combinazioni di chiavi per decrittare il file protetto), *Attacco a dizionario* (prova lunghissimi elenchi di parole, nomi e sigle di uso comune in una data lingua), *Attacco all'algoritmo* (prevede la possibilità di intervenire su particolari debolezze matematiche o computazioni dell'algoritmo utilizzato), *Password sniffing* (ruba la password con qualche trucco, facendosela dire con una scusa, o fingendosi responsabili di un servizio assistenza clienti, o della sicurezza).
   Contromisure: per i sistemi informatici sono gli accessi con password elaborate come previsto nel presente documento; per i locali fisici sono le porte con serrature e chiavi custodite e gestite secondo la procedura prevista.
6. **Defacing:** la sostituzione della homepage del sito della scuola con immagini o scritte.
   Contromisure: sistema di accesso al server web con password e controllo quotidiano per pronta sostituzione.
7. **Violazione del diritto d'autore:** copie e/o installazioni di programmi informatici di cui la scuola non possiede regolare licenza; download, illegale e non autorizzato, dal web di file audio e/o video.
   Contromisure: sistema di autorizzazione con limitazioni per l'installazione di programmi software, informazioni agli utenti, controlli periodici.
8. **Crimini informatici:** i sistemi informatici della scuola potrebbero essere utilizzati per compiere crimini informatici con implicazioni di tipo civile e penale: spamming, tentativi d'intrusione, pubblicazione sul web di testi o immagini proibite, ecc.
   Contromisure: sistema di accesso con account e proxy server, in modo tale da impedire alcuni comportamenti illegali e, in ogni caso, risalire all'autore dell'azione non consentita.
9. **Danni all'hardware:** l'elemento più delicato è il disco fisso; se si dovesse danneggiare, a meno di ricorrere a pratiche costosissime sviluppate da centri specializzati, tutti i dati andrebbero persi. Per i luoghi fisici s'intende la rottura delle serrature o delle chiavi.
   Contromisure: per i sistemi informatici si ripristina con copie di back-up; per i luoghi fisici c'è la sostituzione immediata o chiusura con lucchetto della porta o dell'armadio, ovvero il trasporto in un'altra stanza blindata dei dati sensibili o in altro armadio blindato.
10. **Usurpazione di identità:** al momento di stabilire un collegamento alla rete o di ricevere dati, l'utente deduce l'identità del suo interlocutore in funzione del contesto in cui avviene la comunicazione, potrebbe scaricare software maligno da un sito web che si fa passare per fonte affidabile e si potrebbero anche rivelare informazioni riservate alla persona sbagliata.
    Contromisure: controllo sistematico dell'autenticità delle fonti.

11. **IP spoofing:** l'autore dell'attacco sostituisce la propria identità a quella di un utente legittimo del sistema. Viene fatto non per generare intrusione in senso stretto, ma per effettuare altri attacchi. Lo Spoofing si manifesta come attività di "falsificazione" di alcuni dati telematici, come ad esempio di un indirizzo IP o dell'indirizzo di partenza dei messaggi di posta elettronica.
Contromisure: riservatezza di user-id e password costruite come di seguito indicate.
12. **Spamming:** saturazione di risorse informatiche a seguito dell'invio di un elevato numero di comunicazioni tali da determinare l'interruzione del servizio. Ad esempio l'invio di molti messaggi di posta elettronica con allegati provoca, come minimo, la saturazione della casella di posta elettronica e la conseguente non disponibilità a ricevere ulteriori (veri) messaggi.
Contromisure: software specifico.
13. **Incidenti ambientali ed eventi imprevisti:** catastrofi naturali (tempeste, inondazioni, incidenti, terremoti); terzi estranei a qualsiasi rapporto contrattuale con l'operatore o l'utente (ad es. guasti all'hardware o del software dei componenti o dei programmi consegnati); errore umano dell'operatore (compreso il fornitore di servizio) o dell'utente (ad es. problemi di gestione della rete, installazione errata del software).
Contromisure: per i sistemi informatici copie di back-up per il ripristino; per i luoghi fisici ricorso ad altre stanze o armadi.

7.3 VALUTAZIONE DEI RISCHI

Per valutare i rischi si prevede di utilizzare i seguenti livelli:

- **Lieve:** rischio molto basso corrispondente ad una minaccia remota e comunque rapidamente reversibile od ovviabile.
- **Media:** rischio superiore al precedente corrispondente ad una minaccia remota i cui effetti non sono facilmente o totalmente reversibili od ovviabili.
- **Grave:** rischio che occorre assolutamente prevenire con un insieme di contromisure (di natura fisica, logica, etc.) per abbatterlo o contenerlo a livelli accettabili.

Di seguito vengono riportate delle tabelle che riassumono l'analisi dei rischi effettuata per tutte le risorse presenti nell'Istituzione Scolastica.

ISTITUTO TECNICO COMMERCIALE E PER GEOMETRI
" V. PARETO"
Via Annecchino, 252 – 80078 Pozzuoli (NA)
Tel.: 081/8664962; **Fax**: 081/5046777
C. M.: NATD130003; **e–mail**: natd130003@istruzione.it

TABELLA DI ANALISI DEI RISCHI RISORSE HARDWARE

Risorsa	Elemento di Rischio	Livello
Tutti i computer	Uso non autorizzato dell'hardware	grave
Tutti i computer	Manomissione	medio
Tutti i computer	Probabilità/frequenza di guasto	medio
Tutti i computer	Possibilità di sabotaggio	lieve
Tutti i computer	Furto	lieve
Tutti i computer	Intercettazioni delle trasmissioni dati	medio
Tutti i computer	Eventi naturali (allagamenti, terremoti, etc.)	lieve
Tutti i computer	Incendi	medio
Tutti i computer	Guasti ad apparecchiature connesse	medio
Tutti i computer	Black out	medio

TABELLA DI ANALISI DEI RISCHI DEI LUOGHI FISICI

Risorsa	Elemento di Rischio	Livello
Archivio Amministrazione	Possibilità di intrusione, accesso di persone non autorizzate	medio
Archivio Amministrazione	Furto	lieve
Armadi blindati casseforti	Possibilità intrusione / furto	lieve
Armadi, classificatori	Possibilità intrusione / furto	grave
Locali segreteria, presidenza, vicepresidenza, biblioteca	Possibilità di intrusione, accesso di persone non autorizzate	grave
Locali segreteria, presidenza, vicepresidenza, biblioteca	Eventi naturali (allagamenti, terremoti etc.)	grave
Locali segreteria, presidenza, vicepresidenza, biblioteca	Incendi	grave

TABELLA DI ANALISI DEI RISCHI RISORSE DATI

Risorsa	Elemento di Rischio	Livello
Tutte le banche dati	Cancellazione non autorizzata di dati	Grave
Tutte le banche dati	Manomissione di dati	Grave
Tutte le banche dati	Perdita di dati	Grave
Tutte le banche dati	Accesso non autorizzato	Grave
Tutte le banche dati	Incapacità di ripristinare copie di back-up	Lieve

TABELLA DI ANALISI DEI RISCHI RISORSE SOFTWARE

Risorsa	Elemento di Rischio	Livello
Procedure ARGO	Possibilità di accesso non autorizzato a base dati	Grave
Procedure ARGO	Errori software che minacciano l'integrità dei dati, presenza di codice non conforme alle specifiche dei programmi	Lieve
Sistemi Operativi	Possibilità di accesso non autorizzato a base dati	Grave
Internet e posta elettronica	Possibilità di accesso non autorizzato a base dati	Grave
Programmi di masterizzazione CD / back - up	Mancata registrazione dei dati	Grave
Programmi antivirus e di protezione	Mancato aggiornamento dei file di riconoscimento virus	Grave
Programmi Office	Malfunzionamento a livello software	Lieve

7.4 MISURE DI SICUREZZA ADOTTATE O DA ADOTTARE

Di seguito viene riportata la tabella delle misure minime di sicurezza stabilite dall'Istituzione Scolastica.

TABELLA PER L'ADOZIONE DI IDONEE MISURE DI SICUREZZA

Tipologia misura adottata	Descrizione misura
Fisiche	Custodia di dati o copie in armadi chiusi e/o blindati.
	Controllo degli accesi agli uffici di segreteria, sala docenti, archivi e presidenza.
	Utilizzo di contenitori chiusi per l'eventuale trasporto di documenti con dati sensibili.
	Predisposizione di armadi non accessibili da parte di personale non autorizzato.
	Dispositivi antincendio.
	Verifica dei supporti magnetici per le copie.
Logiche	Nomina e indicazione per iscritto degli incaricati.
	Eventuale nomina del responsabile del trattamento della ditta in outsourcing.
	Nomina ed indicazione in forma scritta dell'Amministratore del sistema.
	Nomina ed indicazione in forma scritta del Custode delle credenziali.
	Predisposizione dell'utilizzo di password.
	Controllo dei sistemi informatici con antivirus.
	Installazione di software per firewall.
	Installazione di software per server Proxy.
	Controllo degli accessi alla rete su ogni singolo sistema informatico.
Organizzative	Divulgazione del DPS a tutte le funzione dell'Istituzione Scolastica.
	Prescrizione di linee guida sulla sicurezza a tutti gli incaricati.
	Formazione degli incaricati.
	Istituzione di un piano di verifica e controllo di tutte le misure adottate.
	Distruzione di tutti i supporti magnetici che non devono essere più utilizzati.

8 PROCEDURE RELATIVE ALLE MISURE IMPOSTE DAL DISCIPLINARE TECNICO

8.1 AGGIORNAMENTO DEGLI INVENTARI DELLE RISORSE (BANCHE DATI/ARCHIVI, UFFICI PER IL TRATTAMENTO DEI DATI E SISTEMI DI ELABORAZIONE)

Gli inventari delle risorse sono riportati nel presente documento. Il Responsabile, in collaborazione con l'Amministratore del sistema (se persona diversa) per la parte riguardante l'elaborazione informatica, ha il compito di tenere aggiornati tali inventari specificando tutte le caratteristiche previste. Il Responsabile può avere un registro o modulo, appositamente dedicato e conservato in luogo sicuro, per la rilevazione e l'aggiornamento dei dati richiesti e, successivamente, provvedere entro il termine previsto dalla normativa vigente a modificare il DPS in modo opportuno.

8.2 MISURE DI SICUREZZA CONTRO IL RISCHIO DI DISTRUZIONE O PERDITA DI DATI

8.2.1 Criteri e procedure per garantire l'integrità dei dati

Al fine di garantire l'integrità dei dati contro il rischio di distruzione o perdita, il Responsabile, con il supporto dell'Amministratore del sistema, ha stabilito che la periodicità con cui debbono essere effettuate le copie di sicurezza delle banche di dati trattati è settimanale.

Il back up per i dati contenuti in ARGO viene effettuato in automatico on line in modo criptato secondo quanto previsto dalla relativa procedura.

Viene, quindi, considerato il solo back up dei dati contenuti nelle cartelle di lavoro presenti sul server. Tale tipo di back up viene effettuato dall'amministratore di sistema sul disco doppio presente all'interno del server. Il Responsabile per sicurezza può prevedere di effettuare back up con dispositivi esterni secondo i seguenti criteri attuativi:

1. il tipo di supporto da utilizzare è una pen drive o disco fisso esterno o CD;
2. il numero di copie di back-up da effettuare è almeno 2;
3. le copie di back-up vengono opportunamente identificate (data di effettuazione del back-up e nome della banca dati in esso contenuto) e conservate in cassaforte dall'Amministratore del sistema;
4. l'Amministratore del sistema, alla realizzazione delle nuove copie di back-up, si assicurerà che le vecchie copie vengano opportunamente cancellate;
5. l'incarico dell'operazione di back-up viene riportato per iscritto e accettato;
6. la procedura di attuazione dell'operazione di back-up (istruzioni e comandi necessari per effettuare le copie di back-up) è preparata dall'Amministratore del sistema, è conservata dal Responsabile e data in copia controllata all'incaricato dell'operazione di back-up e all'Amministratore del sistema.

Vengono, inoltre stabilite le seguenti ulteriori misure per la custodia e la conservazione dei supporti utilizzati per il back-up e per gli altri supporti contenenti dati:

1. l'accesso alle copie di back-up è limitato a:
    a. Responsabile;
    b. Amministratore del sistema;
2. gli eventuali supporti di memorizzazione di dati sensibili (hard disk, floppy, CD ROM, dat, ecc.) sono soggetti alle seguenti misure di sicurezza:
    a. i floppy, CD, DAT non più utilizzati devono essere distrutti fisicamente mediante rottura delle parti principali e taglio delle superfici magnetiche (floppy e DAT) alla presenza dell'Amministratore del sistema;
    b. gli hard disk non più utilizzati devono essere distrutti meccanicamente alla presenza dell' Amministratore del sistema;
    c. gli hard disk ancora idonei all'uso, come nel caso di sostituzioni o dismissioni di personal computer, dovranno essere formattati a basso livello alla presenza dell'Amministratore del sistema che dovrà accertare, mediante apposito verbale, la reale cancellazione di tutti i dati;
    d. in generale, è compito dell'Amministratore del sistema fornire agli incaricati istruzioni affinché in nessun caso vengano lasciate copie di back-up delle banche dati, non più utilizzate, senza che ne venga cancellato il contenuto e annullate e rese illeggibili le informazioni in esso registrate.

Tali disposizioni, per l'incaricato preposto, valgono sia per i sistemi in rete sia per i computer stand alone.