



**PROCEDURA DI GESTIONE
MISURE TECNICHE E ORGANIZZATIVE**

PROCEDURA DI IMPLEMENTAZIONE E CONTROLLO DELLE MISURE TECNICHE E ORGANIZZATIVE IN AMBITO INFORMATICO

*Redatto ed applicato ai sensi e per gli effetti di:
Reg.UE 2016/679 – GDPR – General Data Protection Regulation
D. Lgs. 196/2003 così come modificato ed integrato da D. Lgs. 101/2018*

INFORMAZIONI SUL DOCUMENTO	
Data:	01/10/2018
Azienda:	Istituto Comprensivo Della Val Nure Via Francesco Acerbi n. 61 29028 Ponte dell'Olio (PC) C.F. 80010070334
Rif. Doc.:	Procedura di gestione delle misure minime di sicurezza (misure_sicurezza.pdf)
Versione:	01.01
Redatto da:	GALLI DATA SERVICE SRL (DPO)
Revisionato da:	
Approvato da:	<p style="text-align: center;">Istituto Comprensivo Della Val Nure (Titolare del trattamento)</p> <p style="text-align: center;">In persona di: Teresa Andena (Dirigente Scolastica Reggente)</p> <p style="text-align: right;">..... (TIMBRO E FIRMA)</p>



**PROCEDURA DI GESTIONE
MISURE TECNICHE E ORGANIZZATIVE**

SCOPO

La presente procedura è finalizzata a garantire la corretta configurazione ed utilizzo dell'infrastruttura informatica dell'Istituto, in relazione all'implementazione di adeguate misure di sicurezza a protezione dei dati memorizzati.

RIFERIMENTI NORMATIVI

Le configurazioni informatiche sono stabilite in conformità alle seguenti normative:

- **REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (GDPR, General Data Protection Regulation)**

WEB: <http://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32016R0679&from=IT>

- **D.Lgs.196/2003) nella sua versione novellata.**

WEB: <http://www.garanteprivacy.it/codice>

Si tiene inoltre conto delle indicazioni di ulteriori normative, atte a garantire un adeguato livello di sicurezza dei sistemi informativi e reti di telecomunicazioni aziendali:

- la **Legge 23/12/1993 N°547** "Modificazioni ed integrazioni alle norme del Codice Penale e del codice di procedura penale in tema di criminalità informatica;
- la **Legge 03/08/1998 N°269** "Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme della riduzione in schiavitù" volta al contrasto della detenzione, scambio e commercio di materiale pedopornografico in rete;
- la **Legge 18/08/2000 N°248** "Nuove norme a tutela del Diritto d'Autore" volta a reprimere i comportamenti illeciti di pirateria informatica;
- il **Decreto Legislativo 08/06/2001 N°231** "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'art.11 della Legge 29/09/2000 N°300 per gli aspetti relativi ai crimini informatici

**PROCEDURA DI GESTIONE
MISURE TECNICHE E ORGANIZZATIVE****OGGETTO DELLA POLICY**

Lo scopo previsto in premessa è perseguito, in concreto, attraverso le attività previste nella seguente tabella:

ATTIVITA'	DESCRIZIONE	RIF.LEGGE
Procedure di autenticazione ed autorizzazione	Occorre impostare accorgimenti tecnici atti a garantire che l'accesso alle informazioni sia consentito esclusivamente a soggetti identificati ed autorizzati (in base alle mansioni lavorative)	Artt. 4, 32, GDPR
Strumenti a protezione dell'infrastruttura	Occorre installare adeguati strumenti finalizzati a: <ul style="list-style-type: none">• proteggere i dati contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale (malware informatico)• prevenire le vulnerabilità e correggere i difetti dei sistemi operativi• proteggere i dati contro l'accesso abusivo (intrusione), di cui all'art. 615-ter del codice penale	Artt. 4, 32, GDPR
Politica di back-up dei dati	Prevenire i rischi derivanti dalla perdita di dati, in relazione a eventi naturali o artificiali che potrebbero causarne la cancellazione o la distruzione.	Artt. 4, 32, GDPR

SOGGETTI COINVOLTI

I soggetti coinvolti nella corretta applicazione della procedura sono i seguenti:

SOGGETTO	ATTIVITA'
Titolare (Istituto Comprensivo Statale di Cadeo e Pontenure)	<ul style="list-style-type: none">• Definire le linee guida in materia di: profili di autorizzazione degli utenti, misure di sicurezza a tutela dei dati, politiche di back-up e ripristino• Verificare periodicamente l'attuazione e l'efficacia della procedura
DPO	<ul style="list-style-type: none">• Dare esecuzione alle direttive del Titolare specificate nella presente procedura e lettera di incarico a DPO• Diramare corrette istruzioni agli altri soggetti• Coadiuvare gli utenti
Consulenti esterni (Fornitori servizi informatici)	<ul style="list-style-type: none">• Dare esecuzione alle direttive del Titolare e del DPO
Utenti (Personale che utilizza strumenti elettronici)	<ul style="list-style-type: none">• Utilizzare gli strumenti in conformità della presente e delle istruzioni ricevute



**PROCEDURA DI GESTIONE
MISURE TECNICHE E ORGANIZZATIVE**

ELENCO DEGLI STRUMENTI TECNOLOGICI UTILIZZATI DALL'ISTITUTO:

STRUMENTI TECNOLOGICI	
Tipologia	Descrizione strumento
Strumentazione hardware	pc e server in rete, mobile device
Sistemi operativi	windows, android
Software di protezione	antivirus, firewall
Software segreteria	software per la gestione delle attività di segreteria
Software ministeriali	software per le comunicazioni telematiche
Software di gestione documentale	pacchetti office
Registro digitale	contiene la gestione delle valutazioni degli alunni, offre anche la possibilità di seguire l'andamento scolastico dei propri figli, gli argomenti svolti a scuola, avere traccia delle assenze o dei compiti assegnati.

MODALITA' DI IMPLEMENTAZIONE DELLE MISURE DI SICUREZZA:

MISURE TECNOLOGICHE		
AREA	DESCRIZIONE ED EVIDENZE	PERIMETRO
Autenticazione ed autorizzazione	Le password sono conosciute esclusivamente dagli utenti; hanno almeno 8 caratteri; variano ogni 3 mesi; in caso di assenza dell'utente e di necessità, le password possono essere resettate e ne viene data notizia all'utente che la reimposterà al suo rientro	tutti i dati
	Le password di accesso dei pc, dei gestionali e della posta sono gestite	tutti i dati
Sicurezza perimetrale e difesa malware	Tutti i device sono protetti in tempo reale tramite antivirus	tutti i dati
	La rete è protetta da firewall, con software di controllo dei contenuti (web blocker)	tutti i dati
Sicurezza fisica	l'accesso agli uffici è controllato e presidiato	uffici



**PROCEDURA DI GESTIONE
MISURE TECNICHE E ORGANIZZATIVE**

Misure organizzative	gli accessi degli utenti ai dati sono differenziati	tutti i dati
Consapevolezza e formazione	si è distribuito apposito documento di istruzione	tutti gli incaricati
Backup	Tutti i dati sono oggetto di backup: il backup è gestito in modo conforme alla normativa	tutti i dati
Smaltimento rifiuti elettronici	Tutti i device vengono formattati a basso livello prima di essere passati ad altri utenti; in caso di smaltimento i device sono alternativamente, o formattati, oppure viene distrutta l'unità interna di memoria	tutti i device contenenti dati di tipo personale
Wi.fi	La scuola è dotata di una rete wifi protetta utilizzabile esclusivamente per attività istituzionali e didattiche	Tutti i device abilitati