GDPR SCUOLA

LO STAFF TECNICO DEL DIRIGENTE

MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE ADOTTATE, AI SENSI DELL'ART. 32 DEL GDPR, DALL'ISTITUTO COMPRENSIVO SAN DAMIANO D'ASTI

- **Verbale Audit del 29.09.2021** -

Ai sensi dell'art. 32 del Regolamento Europeo 2016/679 la Scuola, "tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche", deve implementare e mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio.

Le misure di sicurezza sono costituite dal complesso di misure volte a ridurre al minimo i rischi di distruzione o perdita dei dati, accesso non autorizzato, trattamento non consentito e modifica dei dati.

In questo documento vengono indicate le misure di sicurezza che sono state adottate per la protezione dei dati personali dell'Istituto Comprensivo San Damiano D'Asti:

- Misure specifiche per la protezione dei dati

Misura	Office	Cartaceo
Minimizzazione della quantità di dati personali *Descrizione:* *Misure volte a gestire solo dati personali adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.*	La scuola applica il principio di minimizzazione richiedendo solo dati adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.	Vengono trattati i dati degli utenti in moda da rispettare il principio di minimizzazione.
Partizionamento dei dati *Descrizione:* *Misure volte a separare le aree di archiviazione dei dati personali trattati al fine di ridurre la possibilità che i dati possano essere correlati e compromessi, ad esempio attraverso la creazione di cartelle di rete condivise distinte per tipologia di dati personali o l'archiviazione di documentazione cartacea in faldoni o archivi separati.*	I dati vengono partizionati in cartelle di rete condivise sul server. Inoltre i documenti vengono altresì protocollati con protocollo riservato o ordinario. Inoltre i documenti vengono altresì protocollati con protocollo riservato o ordinario nonché archiviati in	I dati vengono suddivisi in faldoni o archivi separati. I documenti cartacei contenenti dati altamente sensibili vengono conservati in cassaforte.

	cloud tramite il programma della segreteria digitale.	
Cifratura *Descrizione:* *Misure volte ad assicurare la riservatezza dei dati personali archiviati (in database, documenti e archivi elettronici, etc.) o trasmessi attraverso le reti (ad es., VPN, HTTPS, TLS, etc.) e per gestire chiavi crittografiche.*	Il sito della scuola è in https ed inoltre vengono adottate tecniche di cifratura in quanto proprie degli strumenti informatici e delle piattaforme utilizzate dalla scuola. Anche la posta è protetta da un protocollo TLS.	No
Pseudonimizzazione *Descrizione:* *Misura tecnica volta a rendere anonimi e non riconducibili alla persona i dati personali trattati attraverso sistemi informatici, ad esempio attraverso l'uso di identificativi numerici in sostituzione del nome e cognome della persona.*	La scuola non adottata questa misura.	Non applicabile al cartaceo
Controllo degli accessi logici ed autenticazione *Descrizione:* *Misure volte ad attuare e implementare la politica di controllo degli accessi logici ai dati personali trattati attraverso sistemi informatici (ad es., politiche di accesso ad applicativi o a cartelle di rete condivise), secondo ruoli e responsabilità definite e profili personali attribuiti agli utenti. Tale politica si basa sul principio della minima conoscenza: ogni utente ha accesso ai soli dati personali strettamente necessari per lo svolgimento dei propri compiti.*	Gli accesi a tutti i programmi che utilizza la scuola, dal registro elettronico alla segreteria digitale, sono controllati attraverso l'impostazione di accessi limitati a cui si accede tramite credenziali e profilo personali. Il personale di segreteria in base al ruolo e al compito che svolge riceve le password e gli identificativi per l'accesso agli applicativi e ai programmi per la	Difficilmente applicabile per i documenti cartacei

	gestione amministrativa della scuola. Inoltre anche l'accesso alla rete è protetto e per accedere ai pc della segreteria è necessario conoscere specifica password a disposizione del solo utente. Le password scelte devono essere complesse e il proprietario ne deve avere cura. Tra l'altro le password vengono aggiornate periodicamente. Anche l'accesso al server è sottoposto a specifico controllo e protetto da password.	
Cancellazione sicura *Descrizione:* *Misura adottata allo scopo di eliminare e distruggere irreversibilmente i dati personali, ad esempio attraverso la smagnetizzazione di un supporto informatico o la distruzione di documenti cartacei, in modo che non possano essere recuperati dal supporto su cui sono archiviati.*	I computer non più in uso se riutilizzati o consegnati in comodato alle famiglie vengono formattati e ripuliti. Si segnala che nei pc degli utenti della segreteria non devono essere salvati e conservati documenti contenenti dati personali (i medesimi documenti devono essere salvati sulla cartella del server). In caso di dismissione del server verrà privato del disco e l'hard disk verrà	I documenti cartacei vengono distrutti ed eliminati tramite il trita documenti.

	conservato dalla scuola o smagnetizzato.	

- Misure generali di sicurezza fisica e logica

Misura	Office	Cartaceo
Sicurezza dell'ambiente operativo *Descrizione:* *Misure adottate per gestire la configurazione di sicurezza di server e database che costituiscono la spina dorsale del sistema di elaborazione dei dati personali, applicando politiche specifiche in funzione della rilevanza dei dati personali trattati dall'applicazione ospitata. Tali misure si applicano anche alla protezione delle applicazioni, in particolare di quelle Web.*	Ogni pc è dotato di nome utente e password personale (non tutti posso accedere ai pc); ed anche l'accesso alle risorse di rete è controllato e consentito solo al personale di segreteria. Le password vengono aggiornate periodicamente. Viene consigliato al personale di scegliere password complesse e ne deve avere cura non diffondendole. Per accedere al server è necessaria una specifica password in possesso dell'assistente amministrativo e della ditta informatica designata che si occupano della gestione della rete. Inoltre il server è posto in un apposito locale, in segreteria, chiuso a chiave.	Non applicabile

	Specifiche misure per la configurazione di sicurezza di server e database vengono adottate congiuntamente dalla scuola dalla ditta informatica incaricata alla gestione e manutenzione della rete.	
Sicurezza della rete e delle comunicazioni *Descrizione:* *Misure adottate per proteggere i dati personali durante il transito attraverso la rete, sia per le connessioni esterne (Internet), sia per l'interconnessione con i sistemi del MIUR.* *A seconda della tipologia di canale sul quale il trattamento è effettuato, gli strumenti di protezione adottati comprendono: firewall, sonde di rilevamento intrusione e altri dispositivi attivi o passivi di sicurezza della rete, protocolli di cifratura, politiche di controllo dei cookies, etc.*	I dati vengono scambiati con il sito del Ministero dell'Istruzione e con il SIDI che sono protetti da https. Anche il sito della scuola è in https. Le comunicazioni tramite email vengono gestite esclusivamente con la pec o la peo istituzionale. I pc della scuola che utilizza la segreteria per lo scambio di dati sono dotati di antivirus e antimalware. Inoltre la scuola ha impostato un firewall di rete (DA VERIFICARE). La connessione alla rete internet di segreteria è indipendente e autonoma rispetto a quella della didattica.	Non applicabile
Tracciatura e monitoraggio *Descrizione:*	DA VERIFICARE SE: Attualmente le operazioni svolte dal	Non applicabile

Misure per la registrazione delle attività eseguite su sistemi informatici dagli utenti e dagli amministratori di sistema su dati personali e sistemi di sicurezza, al fine di consentire il tracciamento delle operazioni svolte. Il monitoraggio delle registrazioni prodotte (c.d. "file di log"), inoltre, consente l'identificazione di potenziali tentativi interni o esterni di violazione del sistema e la rilevazione tempestiva di incidenti relativi a dati personali (ad es., eventi di diffusione, modifica o distruzione non autorizzate di dati personali), fornendo al tempo stesso gli elementi di prova nel contesto delle indagini	personale all'interno della rete non vengono tracciate. OPPURE SE: Ogni utente ha un log numerato e ogni operazione fatta all'interno della rete è tracciata. Anche gli ingressi della ditta esterna che gestisce la rete informatica della scuola sistema sono tracciati. Inoltre i sistemi operativi gestiti dai fornitori esterni di gestionali scolastici su piattaforme cloud registrano gli event-log. Gli accessi degli utenti sono perciò monitorati e ciò è garantito dall'univocità delle credenziali assegnate ad ogni utente utilizzatore.	
Gestione sicura del cambiamento *Descrizione:* *Esistenza ed attuazione di un processo operativo di gestione sicura del cambiamento al fine di controllare, attraverso verifiche e approvazioni, le modifiche eseguite nel sistema IT utilizzato per il trattamento dei dati personali. Ogni modifica deve essere registrata e la data/orario dell'ultima modifica deve essere conservata*	Il personale ha il controllo sul proprio pc e può effettuare gli aggiornamenti dei programmi ma per istallare programmi ma i medesimi devono essere necessari per lo svolgimento del lavoro. Il download di materiale da internet è libero e non sottoposto a restrizioni, ma soggetto comunque a controllo da parte	Non applicabile

	di software antivirus. Oppure il personale non è utente amministratore della macchina e per ogni modifica al sistema e per ogni nuova installazione è necessario l'intervento dell'amministratore di rete??	
Gestione sicura dell'hardware, delle risorse e dei dispositivi *Descrizione:* *Misure adottate per gestire l'inventario e la configurazione di sicurezza dell'hardware, delle risorse di rete e dei dispositivi (server, periferiche, dispositivi di comunicazione, etc.) utilizzati per il trattamento dei dati personali.*	Tutti i computers della scuola sono inventariati. I pc vengono controllati su richiesta del personale. Periodicamente l'assistente amministrativo appositamente incaricato dalla scuola controlla che il server ed i pc al fine siano configurati in modo sicuro.	Non applicabile
Gestione sicura delle postazioni di lavoro *Descrizione:* *Misure adottate per gestire la configurazione di sicurezza delle postazioni di lavoro degli utenti fisse e portatili (ad es., impostazioni del sistema operativo, applicazioni, software di office automation, etc.). Tali politiche impediscono agli utenti di eseguire azioni che potrebbero compromettere la sicurezza del sistema IT (ad es., la disattivazione di programmi antivirus o l'installazione e l'esecuzione di software non autorizzato, accesso a siti potenzialmente pericolosi).*	I computer sono oggetto di periodica verifica da parte l'assistente amministrativo appositamente incaricato dalla scuola che adotta le precauzioni di sicurezza necessarie. Inoltre tutti gli interventi sui pc che potrebbero compromettere la sicurezza del sistema IT sono gestiti dalla ditta informatica incaricata. Su tutti i	Non applicabile

	pc della segreteria è istallato e/o aggiornato l'antivirus. Il personale inoltre rispettare specifiche politiche nello svolgimento del proprio lavoro come quella di bloccare lo schermo del computer in caso di allontanamento (lock screen). La rete è protetta da un firewall che blocca l'accesso a siti potenzialmente pericolosi ed eventuali minacce.	
Backup e Continuità operativa *Descrizione:* *Esistenza ed attuazione di politiche che stabiliscono le modalità di salvataggio dei dati personali, allo scopo di assicurarne la disponibilità e l'integrità nel tempo, e di ripristino dell'operatività a seguito di un evento avverso, ossia le procedure operative e le misure tecniche da seguire per ripristinare la disponibilità e l'accesso ai servizi essenziali in caso di incidente che ne pregiudichi l'operatività.*	Il personale deve lavorare salvando i documenti prodotti nelle cartelle di rete sul server e su tali dati viene effettuato il backup (da definire ogni quanto e dove??) per permettere di ripristinare la disponibilità e l'accesso alle informazioni in caso di incidenti che potrebbero pregiudicarne la disponibilità. I documenti digitali vengono altresì archiviati e conservati in cloud tramite i gestionali utilizzati dalla scuola.	Non applicabile
Manutenzione delle apparecchiature	Vengono svolti, su	Non applicabile

Descrizione: *Esistenza e attuazione di politiche per la manutenzione periodica delle apparecchiature di continuità elettrica, dei sistemi antincendio e di ogni altra tipologia di sistema a supporto dell'operatività dei sistemi informativi*	segnalazione e richiesta del personale, controlli sulle apparecchiature come i gruppi di continuità del server. Periodicamente vengono controllati gli estintori nei locali scolastici.	
Protezione dalle fonti di rischio ambientali *Descrizione:* *Misure adottate per ridurre o contenere i rischi connessi a minacce ambientali (fenomeni climatici, incendi, allagamenti) che potrebbero influire sull'operatività dei sistemi informativi, sulla continuità dei servizi erogati e sulla sicurezza dei dati personali trattati. Esempi sono: gruppi di continuità, sistemi antincendio, armadi ignifughi, etc.*	Le minacce ambientali sono oggetto di valutazione e di protezione da parte del RSPP, inoltre la scuola utilizza gruppi di continuità per il server nonché sono presenti nei locali scolastici degli estintori.	Le minacce ambientali sono oggetto di valutazione e di protezione da parte del RSPP, inoltre sono a disposizione in caso di incendio degli estintori.

- Misure organizzative e processi di governo

Misura	Office	Cartaceo
Modello Organizzativo e di Gestione *Descrizione:* *Il modello organizzativo e di gestione della privacy costituisce il fondamento per la sicurezza dei dati personali trattati dall'organizzazione, definendo i processi volti a controllare i rischi che i trattamenti dell'organizzazione pongono sui diritti e le libertà delle persone interessate e individuando ruoli e responsabilità di chi ha accesso ai dati personali, in base al principio del minimo privilegio. Un ruolo di particolare importanza è svolto dal Responsabile della*	E' stato definito un organigramma privacy. Tutto il personale è stato designato autorizzato al trattamento dei dati personali e ha ricevuto le istruzioni su come trattare i dati. La scuola ha poi provveduto a nominare il Dott. Federico Croso quale	E' stato definito un organigramma privacy. Tutto il personale è stato designato autorizzato al trattamento dei dati personali e ha ricevuto le istruzioni su come trattare i dati. La scuola ha poi provveduto a nominare il Dott. Federico Croso quale

Protezione dei Dati (RPD), che monitora la conformità al regolamento e collabora con il Titolare nell'adeguare le misure di protezione dei dati personali trattati.	proprio responsabile della protezione dei dati. Il titolare del trattamento ha, inoltre, redatto il registro delle attività, ai sensi dell'art. 30 del GDPR.	proprio responsabile della protezione dei dati. Il titolare del trattamento ha, inoltre, redatto il registro delle attività, ai sensi dell'art. 30 del GDPR.
Politiche e procedure per la protezione dei dati personali *Descrizione:* *La politica per la protezione dei dati personali dimostra l'impegno generale alla protezione dei dati personali e definisce i principi di base per la loro sicurezza e protezione. Il documento formalizza gli obiettivi e le regole da applicare nel campo della protezione dei dati e costituisce la base per l'attuazione delle misure tecniche e organizzative specifiche richieste dall'art. 32 del RGPD. Le specifiche misure tecniche e organizzative attuate sono descritte in procedure operative di dettaglio che indirizzano temi specifici (ad esempio controllo degli accessi, gestione dei dispositivi, gestione delle risorse, ecc.).*	Il personale è stato formato in merito agli adempimenti da porre in essere per proteggere i dati degli interessati. E' stata adottata una politica sulla protezione dei dati. La scuola ha redatto per ciascun trattamento le specifiche informative privacy. Infine, sono state analizzate le misure tecniche e organizzative implementate e previste delle check list relative agli adempimenti in materia di privacy e di sicurezza per i dati.	Il personale è stato formato in merito agli adempimenti da porre in essere per proteggere i dati degli interessati. E' stata adottata una politica sulla protezione dei dati. La scuola ha redatto per ciascun trattamento le specifiche informative privacy. Infine, sono state analizzate le misure tecniche e organizzative implementate e previste delle check list relative agli adempimenti in materia di privacy e di sicurezza per i dati.
Gestione dei Responsabili del trattamento e delle terze parti *Descrizione:* *I rapporti con fornitori esterni di servizi che hanno accesso a o trattano dati personali per conto del Titolare devono essere formalizzati tramite un contratto o altro atto legale stabilito e siglato tra le parti, in cui è disciplinato il trattamento da parte del responsabile e specificate le misure tecniche e organizzative adottate nel rispetto dei*	I responsabili del trattamento sono stati identificati e nominati.	I responsabili del trattamento sono stati identificati e nominati.

requisiti del RGPD e a garanzia della tutela dei diritti dell'interessato.		
Sicurezza del ciclo di vita delle applicazioni e nei progetti *Descrizione:* *Misure specifiche predisposte per garantire che si considerino i requisiti di protezione dei dati personali e l'applicazione delle più severe impostazioni sulla privacy sin dalle prime fasi del processo di sviluppo di un sistema informativo e durante il ciclo di vita delle applicazioni, nel rispetto dei principi di "Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita" introdotti dall'art. 25 del RGPD.*	Tutti i sistemi dal registro elettronico alle piattaforme utilizzate sono implementate secondo le raccomandazioni del GDPR e dell'AgID. I fornitori dei servizi devono infatti garantire alla scuola l'adesione alle attuali norme in materia di trattamento dei dati	Non applicabile
Gestione degli Incidenti di sicurezza e delle Violazioni dei dati personali *Descrizione:* *Nel caso si verifichino incidenti di sicurezza che comportano la "distruzione, perdita, modifica, divulgazione non autorizzata o accesso ai dati personali trasmessi, conservati o comunque trattati" (cfr. art. 4.12 del RGPD), sono attivate procedure per la gestione di tali eventi e la notifica all'autorità di controllo e alle persone interessate.*	Adozione di una procedura per gestione data breach e predisposizione di registro delle violazioni.	Adozione di una procedura per gestione data breach e predisposizione di registro delle violazioni.
Gestione e formazione del personale *Descrizione:* *Misure specifiche predisposte per garantire che il personale coinvolto nel trattamento dei dati personali sia adeguatamente informato in merito agli obblighi di riservatezza, specialmente per il personale chiave coinvolto nel trattamento dei dati personali ad alto rischio, e sensibilizzato sulle procedure di sicurezza e protezione dei dati (ad esempio uso di password e accesso a specifici sistemi di elaborazione e trasmissione dati).*	Nomine persone autorizzate e formazione.	Nomine persone autorizzate e formazione.
Controllo degli accessi fisici	I collaboratori scolastici sono	I collaboratori scolastici sono

Descrizione: *Misure volte ad assicurare la sicurezza fisica e il controllo degli accessi agli edifici e alle zone in cui sono ospitate le risorse a supporto del trattamento (documenti cartacei e strumenti informatici), ad esempio attraverso un servizio di portineria, l'uso di tornelli con autenticazione tramite badge di riconoscimento e porte chiuse a chiave.*	incaricati di monitorare le entrate e le uscite. Tutti gli ingressi vengono annotati in un apposito registro dei visitatori esterni. L'accesso ai locali della segreteria è consentito solo se il personale è presente.	incaricati di monitorare le entrate e le uscite. Tutti gli ingressi vengono annotati in un apposito registro dei visitatori esterni. L'accesso ai locali della segreteria è consentito solo se il personale è presente.
Sicurezza dei documenti cartacei *Descrizione:* *Politiche e processi di gestione dell'archivio per assicurare che i documenti cartacei contenenti dati personali utilizzati durante il trattamento siano prodotti, archiviati, consultati, trasmessi e distrutti nel rispetto dei diritti dell'interessato.*	Non applicabile	I documenti cartacei, per prassi, vengono conservati nell'archivio corrente all'interno dell'ufficio della segreteria in armadi; l'ingresso ai locali è monitorato dal personale presente. In caso di assenza del personale gli uffici vengono chiusi a chiave. I documenti altamente sensibili e i fascicoli riservati sono custoditi in cassaforte. I documenti non più in uso vengono archiviati in un apposito locale, chiuso a chiave, a norma di legge e dotato di porta tagliafuoco il cui accesso è consentito al solo personale autorizzato. La scuola ha previsto, poi, un secondo archivio storico negli uffici e tutti i documenti sono

		contenuti in armadi chiusi a chiave.