VALUTAZIONE DEL RISCHIO E MISURA DI SICUREZZA PER IL TRATTAMENTO DEI DATI PERSONALI

Valutazione del livello di rischio per le operazioni di trattamento **Archiviazione pubblico interesse** e proposta di adeguate misure di sicurezza tecniche e organizzative.

Sezione I – Definizione e contesto del trattamento

DESCRIZIONE DELL'OPERAZIONE DI TRATTAMENTO	RISPOSTA	
Dati personali trattati	Alcuni dei dati personali comuni e particolari cui la scuola è a conoscenza e conserva sui propri sistemi in virtù del rapporto con gli interessati e comunque la cui conservazione in archivio è richiesta secondo il piano di conservazione e scarto per gli archivi delle istituzioni scolastiche.	
Finalità del trattamento	Archiviazione dati nel rispetto delle " Regole deontologiche per il trattamento a fini di archiviazione"	
Soggetto dei dati	Potenzialmente tutti coloro che hanno rapporti con la scuola	
Mezzi di trattamento	Trattamento cartaceo e Trattamento elettronico	
Destinatari dei dati personali	Interno	Personale autorizzato
	Esterno	
Responsabile del trattamento utilizzato		

Sezione II – Valutazione dell'impatto

Valutazione dell'impatto sulla riservatezza: Bassa

Valutazione dell'impatto dell'integrità: Bassa

Valutazione dell'impatto della bassa disponibilità : Bassa

VALUTAZIONE D'IMPATTO		
Riservatezza	**Integrità**	**Disponibilità**
Basso	Basso	Basso
	Valutazione d'impatto globale	Basso

Sezione III – Analisi delle minacce per area di valutazione

Probabilità di minaccia delle risorse tecniche e di rete: bassa

- **Fa parte del trattamento dei dati personali attraverso Internet? Sì**
- **È possibile fornire l'accesso a un sistema interno di trattamento dei dati personali tramite Internet (ad esempio per determinati utenti o gruppi di utenti)? Sì**
- **Il sistema di trattamento dei dati personali è interconnesso a un altro sistema o servizio IT esterno o interno (alla tua organizzazione)? Sì**
- **Le persone non autorizzate possono accedere facilmente all'ambiente di elaborazione dei dati? No**
- **Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza seguire le migliori pratiche documentate pertinenti? No**

Processi/Procedure relativi al trattamento dei dati personali probabilità di minaccia: Bassa

- **I ruoli e le responsabilità in relazione al trattamento dei dati personali sono vaghi o non chiaramente definiti? No**
- **L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito? No**
- **I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali? No**
- **I dipendenti sono autorizzati a trasferire, archiviare o altrimenti elaborare dati personali al di fuori dei locali dell'organizzazione? No**
- **Le attività di trattamento dei dati personali possono essere eseguite senza creare file di log?**

Nessuna

Parte/Persone coinvolte nel trattamento dei dati personali probabilità di minaccia: Bassa

- **Il trattamento dei dati personali viene effettuato da un numero indefinito di dipendenti? No**
- **Fa parte dell'operazione di trattamento dei dati eseguita da un appaltatore/terza parte (responsabile del trattamento dei dati)? No**
- **Gli obblighi delle parti/persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente indicati? No**
- **Il personale coinvolto nel trattamento dei dati personali non ha familiarità con le questioni di sicurezza? No**
- **Le persone/le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e/o distruggere in modo sicuro i dati personali? No**

Settore di attività e scala della probabilità di minaccia di elaborazione : bassa

- **Ritiene che il vostro settore di attività sia soggetto ad attacchi informatici? No**
- **La tua organizzazione ha subito attacchi informatici o altri tipi di violazione della sicurezza negli ultimi due anni? No**
- **Hai ricevuto segnalazioni e/o reclami in merito alla sicurezza del sistema informatico (utilizzato per il trattamento dei dati personali) nell'ultimo anno? No**
- **Il trattamento riguarda un grande volume di persone e/o dati personali? No**
- **Esistono best practice di sicurezza specifiche per il tuo settore di attività che non sono state seguite adeguatamente? Sì**

AREA DI VALUTAZIONE	PROBABILITÀ	
Rete e risorse tecniche	Basso	1
Processi/Procedure connessi al trattamento dei dati personali	Basso	1
Soggetti/Soggetti coinvolti nel trattamento dei dati personali	Basso	1
Settore di attività e scala di lavorazione	Basso	1
Probabilità complessiva di accadimento della minaccia	Bassa (4)	

Sezione IV – Valutazione del rischi

	LIVELLO DI IMPATTO			
PROBABILITÀ DI **ACCADIMENTO** DELLA MINACCIA		Basso	Medio	Alto / Molto Alto
	Basso	X		
	Medio			
	Alto			

Sezione V – Misure di sicurezza organizzative

Va osservato che l'adeguatezza delle misure al rischio specifico I livelli non dovrebbero essere percepiti come assoluti. A seconda del contesto del trattamento dei dati personali, l'organizzazione può considerare adottare misure aggiuntive, anche se assegnate a un livello di rischio. Inoltre, l'elenco di misure proposto non tiene conto altri requisiti di sicurezza specifici del settore, nonché normative specifiche obblighi, derivanti ad esempio dalla direttiva ePrivacy o dalla direttiva NIS. Nel tentativo di facilitare ulteriormente questa procedura, una mappatura del gruppo proposto di sono incluse anche misure con i controlli di sicurezza ISO/ IEC 27001:2013.

Politica e procedure di sicurezza per la protezione dei dati personali

Identificatore di misura	Descrizione della misura	Livello di rischio
A.1	L'organizzazione dovrebbe documentare la propria politica in materia di trattamento dei dati personali come parte della propria politica di sicurezza delle informazioni.	
A.2	La politica di sicurezza dovrebbe essere riesaminata e rivista, se necessario, su base annuale.	
	Correlati a ISO 27001:2013 - A.5 Politica di sicurezza	

Ruoli e responsabilità

Identificatore di misura	Descrizione della misura	Livello di rischio
B.1	I ruoli e le responsabilità relativi al trattamento dei dati personali dovrebbero essere chiaramente definiti e assegnati conformemente alla politica di sicurezza.	
B.2	Durante le riorganizzazioni interne o le cessazioni e il cambiamento di impiego, la revoca dei diritti e delle responsabilità con le rispettive procedure di consegna dovrebbe essere chiaramente definita.	
	Correlati a ISO 27001:2013 - A.6.1.1 Ruoli e responsabilità in materia di sicurezza delle informazioni	

Politica di controllo degli accessi

Identificatore di misura	Descrizione della misura	Livello di rischio
C.1	A ciascun ruolo (coinvolto nel trattamento dei dati personali) dovrebbero essere assegnati diritti specifici di controllo dell'accesso secondo il principio della necessità di sapere.	
	Correlati a ISO 27001:2013 - A.9.1.1 Politica di controllo degli accessi	

Gestione delle risorse/delle risorse

Identificatore di misura	Descrizione della misura	Livello di rischio
D.1	L'organizzazione dovrebbe disporre di un registro delle risorse informatiche utilizzate per il trattamento dei dati personali (hardware, software e rete). Il registro potrebbe contenere almeno le seguenti informazioni: risorsa informatica, tipo (ad esempio server, workstation), ubicazione (fisica o elettronica). A una persona specifica dovrebbe essere assegnato il compito di mantenere e aggiornare il registro (ad esempio il responsabile informatico).	
D.2	Le risorse IT dovrebbero essere riviste e aggiornate regolarmente.	
	Correlati alla ISO 27001:2013 - A.8 Gestione patrimoniale	

Gestione delle modifiche

Identificatore di misura	Descrizione della misura	Livello di rischio
E.1	L'organizzazione dovrebbe assicurarsi che tutte le modifiche al sistema IT siano registrate e monitorate da una persona specifica (ad esempio IT o responsabile della sicurezza). Dovrebbe essere effettuato un monitoraggio regolare di questo processo.	
E.2	Lo sviluppo del software deve essere eseguito in un ambiente speciale che non sia collegato al sistema informatico utilizzato per il trattamento dei dati personali. Quando è necessario eseguire il test, è necessario utilizzare dati fittizi (non dati reali). Nei casi in cui ciò non sia possibile, dovrebbero essere predisposte procedure specifiche per la protezione dei dati personali utilizzati nelle prove.	
	Correlati alla ISO 27001:2013 - A. 12.1 Procedure operative e responsabilità	

Responsabili del trattamento

Identificatore di misura	Descrizione della misura	Livello di rischio
F.1	Le linee guida e le procedure formali relative al trattamento dei dati personali da parte dei responsabili del trattamento (appaltatori/esternalizzazione) dovrebbero essere definite, documentate e concordate tra il titolare del trattamento e il responsabile del trattamento prima dell'inizio delle attività di trattamento . Queste linee guida e procedure dovrebbero stabilire obbligatoriamente lo stesso livello di sicurezza dei dati personali richiesto nella politica di sicurezza dell'organizzazione.	
F.2	Qualora venga a conoscenza di una violazione dei dati personali, il responsabile del trattamento informa il titolare del trattamento senza indebito ritardo.	
F.3	I requisiti e gli obblighi formali dovrebbero essere formalmente concordati tra il titolare del trattamento e il responsabile del trattamento dei dati. Il responsabile del trattamento dei dati dovrebbe fornire prove documentate sufficienti della conformità.	
	Correlati a ISO 27001:2013 - A.15 Rapporti con i fornitori	

Gestione degli incidenti / Violazioni dei dati personali

Identificatore di misura	Descrizione della misura	Livello di rischio
G.1	È opportuno definire un piano di risposta agli incidenti con procedure dettagliate per garantire una risposta efficace e ordinata agli incidenti relativi ai dati personali.	
G.2	Le violazioni dei dati personali devono essere segnalate immediatamente alla direzione. Dovrebbero essere predisposte procedure di notifica per la segnalazione delle violazioni alle autorità competenti e agli interessati, ai sensi degli articoli 33 e 34 del GDPR.	
	Correlati a ISO 27001:2013 - A.16 Gestione degli incidenti di sicurezza delle informazioni	

Continuità operativa

Identificatore di misura	Descrizione della misura	Livello di rischio
H.1	L'organizzazione dovrebbe stabilire le principali procedure e controlli da seguire al fine di garantire il livello richiesto di continuità e disponibilità del sistema IT che tratta i dati personali (in caso di incidente/ violazione dei dati personali).	
	Correlati alla ISO 27001:2013 - A. 17 Aspetti della sicurezza delle informazioni nella gestione della continuità operativa	

Riservatezza del personale

Identificatore di misura	Descrizione della misura	Livello di rischio
I.1	L'organizzazione dovrebbe garantire che tutti i dipendenti comprendano le loro responsabilità e obblighi relativi al trattamento dei dati personali. I ruoli e le responsabilità dovrebbero essere chiaramente comunicati durante il processo di pre-assunzione e/o di inserimento.	
Correlati a ISO 27001:2013 - A.7 Sicurezza delle risorse umane		

Formazione

Identificatore di misura	Descrizione della misura	Livello di rischio
J.1	L'organizzazione dovrebbe garantire che tutti i dipendenti siano adeguatamente informati sui controlli di sicurezza del sistema IT relativi al loro lavoro quotidiano. I dipendenti coinvolti nel trattamento dei dati personali dovrebbero inoltre essere adeguatamente informati in merito ai pertinenti requisiti in materia di protezione dei dati e agli obblighi giuridici attraverso regolari campagne di sensibilizzazione.	
Correlati a ISO 27001:2013 - A.7.2.2 Sensibilizzazione, istruzione e formazione sulla sicurezza delle informazioni		

Controllo degli accessi e autenticazione

Identificatore di misura	Descrizione della misura	Livello di rischio
K.1	Dovrebbe essere implementato un sistema di controllo degli accessi applicabile a tutti gli utenti che accedono al sistema informatico. Il sistema dovrebbe consentire la creazione, l'approvazione, la revisione e l'eliminazione degli account utente.	
K.2	L'uso di account utente comuni dovrebbe essere evitato. Nei casi in cui ciò sia necessario, è opportuno garantire che tutti gli utenti dell'account comune abbiano gli stessi ruoli e responsabilità.	
K.3	Dovrebbe essere in atto un meccanismo di autenticazione che consenta l'accesso al sistema IT (basato sulla politica e sul sistema di controllo degli accessi). Come minimo dovrebbe essere utilizzata una combinazione nome utente/password. Le password devono rispettare un certo livello (configurabile) di complessità.	
K.4	Il sistema di controllo degli accessi dovrebbe avere la capacità di rilevare e non consentire l'utilizzo di password che non rispettano un certo livello (configurabile) di complessità.	
Correlati a ISO 27001:2013 - A.9 Controllo accessi		

Registrazione e monitoraggio

Identificatore di misura	Descrizione della misura	Livello di rischio
L.1	I file di registro devono essere attivati per ogni sistema/applicazione utilizzata per il trattamento dei dati personali. Dovrebbero includere tutti i tipi di accesso ai dati (visualizzazione, modifica,	

	cancellazione).	
L.2	I file di registro devono essere contrassegnati con data e ora e adeguatamente protetti contro manomissioni e accessi non autorizzati. Gli orologi devono essere sincronizzati con un'unica fonte di tempo di riferimento	
Correlati a ISO 27001:2013 - A.12.4 Registrazione e monitoraggio		

Sicurezza server/database

Identificatore di misura	**Descrizione della** misura	**Livello di** rischio
M.1	I server di database e applicazioni devono essere configurati per l'esecuzione utilizzando un account separato, con privilegi minimi del sistema operativo per funzionare correttamente.	
M.2	I server di database e applicazioni dovrebbero trattare solo i dati personali che sono effettivamente necessari per il trattamento al fine di raggiungere i loro scopi di trattamento.	

Identificatore di misura	Descrizione della misura	Livello di rischio
Correlati alla ISO 27001:2013 - A. 12 Sicurezza delle operazioni		

Sicurezza delle workstation

Identificatore di misura	Descrizione della misura	Livello di rischio
N.1	Gli utenti non dovrebbero essere in grado di disattivare o ignorare le impostazioni di protezione.	
N.2	Le applicazioni antivirus e le firme di rilevamento devono essere configurate su base settimanale.	
N.3	Gli utenti non devono disporre dei privilegi per installare o disattivare applicazioni software non autorizzate.	
N.4	Il sistema dovrebbe avere timeout di sessione quando l'utente non è stato attivo per un certo periodo di tempo.	
N.5	Gli aggiornamenti critici per la protezione rilasciati dallo sviluppatore del sistema operativo devono essere installati regolarmente.	
Correlati alla ISO 27001:2013 - A. 14.1 Requisiti di sicurezza dei sistemi di informazione		

Sicurezza della rete/comunicazione

Identificatore di misura	Descrizione della misura	Livello di rischio
O.1	Ogni volta che l'accesso viene eseguito tramite Internet, la comunicazione deve essere crittografata tramite protocolli crittografici (TLS / SSL).	
Correlati a ISO 27001:2013 - A.13 Sicurezza delle comunicazioni		

Back-up

Identificatore di misura	Descrizione della misura	Livello di rischio
P.1	Le procedure di backup e ripristino dei dati dovrebbero essere definite, documentate e chiaramente collegate ai ruoli e alle responsabilità.	
P.2	I backup dovrebbero ricevere un livello adeguato di protezione fisica e ambientale coerente con le norme applicate ai dati originari.	
P.3	L'esecuzione dei backup deve essere monitorata per garantire la completezza.	
P.4	I backup completi dovrebbero essere eseguiti regolarmente.	
Correlati a ISO 27001:2013 - A.12.3 Back-up		

Dispositivi mobili/portatili

Identificatore di misura	Descrizione della misura	Livello di rischio
D.1	Le procedure di gestione dei dispositivi mobili e portatili dovrebbero essere definite e documentate stabilendo regole chiare per il loro corretto utilizzo.	
Q.2	I dispositivi mobili autorizzati ad accedere al sistema informativo devono essere preregistrati e preautorizzati.	
Q.3	I dispositivi mobili dovrebbero essere soggetti agli stessi livelli di procedure di controllo dell'accesso (al sistema di trattamento dei dati) delle altre apparecchiature terminali.	
	Correlati a ISO 27001:2013 - A. 6.2 Dispositivi mobili e telelavoro	

Sicurezza del ciclo di vita delle applicazioni

Identificatore di misura	Descrizione della misura	Livello di rischio
R.1	Durante il ciclo di vita dello sviluppo dovrebbero essere seguite le migliori pratiche, le pratiche, i quadri o gli standard di sviluppo sicuri e ben riconosciuti.	
R.2	I requisiti di sicurezza specifici devono essere definiti durante le prime fasi del ciclo di vita dello sviluppo.	
R.3	Le tecnologie e le tecniche specifiche concepite per sostenere la tutela della vita privata e la protezione dei dati (note anche come tecnologie che rafforzano la tutela della vita privata (PET)) dovrebbero essere adottate in analogia con i requisiti di sicurezza.	
R.4	Dovrebbero essere seguite norme e pratiche di codifica sicure.	
R.5	Durante lo sviluppo, devono essere eseguiti test e convalida rispetto all'attuazione dei requisiti di sicurezza iniziali.	
	Correlati a ISO 27001:2013 - A.12.6 Gestione delle vulnerabilità tecniche e A.14.2 Sicurezza nei processi di sviluppo e supporto	

Cancellazione/smaltimento dei dati

Identificatore di misura	Descrizione della misura	Livello di rischio
S.1	La sovrascrittura basata su software deve essere eseguita su tutti i supporti prima del loro smaltimento. Nei casi in cui ciò non sia possibile (CD, DVD, ecc.) deve essere eseguita la distruzione fisica.	
S.2	È effettuata la triturazione della carta e dei supporti portatili utilizzati per conservare i dati personali.	
	Correlati a ISO 27001:2013 - A. 8.3.2 Smaltimento dei supporti & A. 11.2.7 Smaltimento sicuro o riutilizzo delle apparecchiature	

Sicurezza fisica

Identificatore di misura	Descrizione della misura	Livello di rischio
T.1	Il perimetro fisico dell'infrastruttura del sistema IT non deve essere accessibile da personale non autorizzato.	
	Correlati alla ISO 27001:2013 - A.11 – Sicurezza fisica e ambientale	