Sistema di gestione integrato
per la qualità e la sicurezza delle informazioni

Politica del sistema di gestione integrato

Note di revisione		
Motivo revisione	**Numero**	**Data**
REV.	1	20/06/2024

Transition from ISO 27001:2013 to ISO 27001:2022 2 07/01/2025 Revisione e allineamento NIS2/D.Lgs. 138/2024 3 29/06/2026

Sommario

1. Introduzione 3 1.1. Recepimento Gruppo 3 2. Scopo e Obiettivi 3 3. Campo di applicazione 4 4. Contenuto della Politica 5 5. Responsabilità 5 6. Aree di Presidio 6 7. Matrice RACI 6 8. Cloud computing 7 9. Riesame 8 10. Eccezioni 8 11. Governance e Applicazione 8 12. Glossario 8

POLITICA DEL SISTEMA DI GESTIONE INTEGRATO

MOD 520 - Rev. 3 del 29/06/2026

1. Introduzione

1.1. Recepimento Gruppo

La presente policy recepisce e contestualizza la Direttiva di Gruppo DYB.GOV.PO.01 "Politica per la Sicurezza delle Informazioni" Rev. 1 del 20/03/2026, adattandola al contesto operativo, normativo e organizzativo di Madisoft S.p.A. in qualità di Soggetto Essenziale ai sensi del D.Lgs. 138/2024.

Madisoft S.p.A. è una software House, certificata SaaS per i servizi Cloud per la Pubblica Amministrazione, che sviluppa e commercializza, per il mondo scuola, i seguenti prodotti a marchio Nuvola: Nuvola Amministrazione Digitale, Nuvola Area Alunni e Registro elettronico, Nuvola Area personale, Nuvola Rilevazione Presenze, Nuvola Sito web scolastico.

Si tratta di prodotti in cloud progettati per la Pubblica amministrazione scolastica (e per gli istituti scolastici ad essa equiparati), accessibili da qualunque dispositivo, fisso o mobile, purché collegati alla rete Internet che consentono di adempiere all'obbligo, variamente declinato, di dematerializzare i propri flussi documentali.

Madisoft S.p.A., data la natura delle proprie attività, considera *la qualità e la sicurezza delle informazioni* un fattore irrinunciabile per la protezione del proprio patrimonio informativo ed un fattore di valenza strategica facilmente trasformabile in vantaggio competitivo.

Per questo motivo, la Direzione di Madisoft S.p.A. ha definito, divulgato e si impegna a mantenere attiva a tutti i livelli della propria organizzazione la presente "politica" per l'implementazione di un *Sistema di Gestione Integrato della Qualità e della Sicurezza delle Informazioni*, comprese le attività svolte tramite "cloud computing".

2. Scopo e Obiettivi

Lo scopo della presente policy è di garantire la qualità dei propri prodotti in accordo con quanto previsto dalla norma **ISO 9001:2015**, nonchè la tutela e la protezione da tutte le minacce, interne o esterne, intenzionali o accidentali, delle informazioni nell'ambito delle proprie attività in accordo con le indicazioni fornite dallo standard **ISO/IEC 27001:2022**, dalle linee guida contenute nello standard **ISO/IEC 27002:2022** e dai requisiti previsti dalle norme **ISO/IEC 27017:2021**, **27018:2020**, **Direttiva (UE) 2022/2555 (NIS2)**, **D.Lgs. 138/2024** e **Determina ACN 164179/2025** nell'ambito del cloud computing. Madisoft adotta un approccio multi-rischio conforme all'Art. 21.1 NIS2, includendo rischi cyber, accidentali, naturali, umani e ambientali.

In questo modo Madisoft S.p.A. vuole garantire un adeguato livello di sicurezza dei dati e delle informazioni nell'ambito della progettazione, sviluppo ed erogazione dei servizi aziendali, attraverso l'identificazione, la valutazione ed il trattamento dei rischi ai quali i servizi stessi sono soggetti.

Il *Sistema di Gestione Integrato Qualità e Sicurezza delle Informazioni* definisce un insieme di misure

organizzative, tecniche e procedurali a garanzia del soddisfacimento dei sottoelencati requisiti di sicurezza di base delle informazioni:

- ***Riservatezza***, ovvero la proprietà dell'informazione di essere nota solo a chi ne ha i privilegi; ● ***Integrità***, ovvero la proprietà dell'informazione di essere modificata solo ed esclusivamente da chi ne possiede i privilegi;

- ***Disponibilità***, ovvero la proprietà dell'informazione di essere accessibile e utilizzabile quando richiesto dai processi e dagli utenti che ne godono i privilegi.

Inoltre, con la presente Politica, Madisoft S.p.A. intende formalizzare i seguenti **obiettivi** nell'ambito della *qualità e della sicurezza delle informazioni*:

- individuare e soddisfare i requisiti dei clienti, utenti e parti interessate;
- sfruttare e rinforzare le opportunità identificate;
- migliorare qualitativamente i servizi identificando e valutando i rischi connessi, nella consapevolezza che questo migliori l'efficacia ed efficienza dei servizi prestati;
- pianificare i propri processi con approccio Risk-Based Thinking (RBT) al fine di attuare le azioni più idonee per valutare e trattare rischi associati;
- identificare le diverse attività come processi da pianificare, controllare e migliorare costantemente e contemporaneamente attivare al meglio le risorse per la loro realizzazione;
- adottare le misure atte a garantire la fidelizzazione del personale e la sua professionalizzazione; ● aumentare, nel proprio personale, il livello di sensibilità e la competenza sui temi della sicurezza; ● determinare e selezionare opportunità di miglioramento;
- promuovere a tutti i livelli un adeguato senso di proattività nella gestione dei propri rischi; ● preservare al meglio l'immagine dell'azienda quale fornitore affidabile e competitivo; ● proteggere il proprio patrimonio informativo, prevenendo divulgazioni accidentali o intenzionali di dati sensibili, proteggendo i dati da modifiche non autorizzate, garantendo che siano accurati e completi e assicurando che le informazioni e i sistemi siano accessibili quando necessario; ● evitare al meglio ritardi nella delivery;
- rispondere pienamente alle indicazioni della normativa vigente e cogente;
- mantenere il sistema di gestione adeguato, efficiente ed efficace al fine d'essere in grado di adattarsi rapidamente al cambiamento delle circostanze e/o dei vincoli esterni all'organizzazione; ● rendere pubblica e accessibile la presente Politica;
- adeguare la presente Politica alle evoluzioni normative di settore e alle esigenze derivanti dai requisiti definiti nel sistema gestione in un'ottica di miglioramento continuo.

3. Campo di applicazione

Questa politica si applica indistintamente a tutte le parti interessate, interne ed esterne all'organizzazione. La sua attuazione è obbligatoria a tutto il personale e deve essere inserita nella regolamentazione degli

accordi con qualsiasi soggetto esterno che, a qualsiasi titolo, possa essere coinvolto con il trattamento di informazioni, l'uso del software di gestione, nonché il servizio di "cloud computing", rientranti nel campo di applicazione del *Sistema di Gestione Integrato Qualità e Sicurezza delle Informazioni* (SGI), ovvero per tutti i dati provenienti dagli applicativi sviluppati dall'azienda.

Madisoft S.p.A. consente la comunicazione e la diffusione delle informazioni verso l'esterno solo per il corretto svolgimento delle attività aziendali che devono avvenire nel rispetto delle regole e delle norme cogenti, nonché delle regole e dei livelli di sicurezza imposti dalla direzione aziendale, nell'ambito della riduzione dei rischi.

4. Contenuto della Politica

Madisoft
Buffetti Group

POLITICA DEL SISTEMA DI GESTIONE INTEGRATO

MOD 520 - Rev. 3 del 29/06/2026

Il SGI si applica a tutte le attività di analisi, progettazione, sviluppo e manutenzione, ai servizi e ai dati ad esse collegate: tutte le informazioni che vengono create o utilizzate da Madisoft S.p.A. sono da salvaguardare e debbono essere protette, secondo la classificazione attribuita, dalla loro creazione, durante il loro utilizzo, fino alla loro eliminazione. Le informazioni debbono essere gestite in modo sicuro, accurato e affidabile e debbono essere prontamente disponibili per gli usi consentiti. È qui da intendersi con "utilizzo dell'informazione" qualsiasi forma di trattamento che si avvalga di supporti elettronici, cartacei o consenta, in una qualsiasi forma, la comunicazione verbale.

Relativamente all'ambito della progettazione e sviluppo, tale sistema prevede – in conformità alla norma **ISO/IEC 27001:2022** – che il ***Security Manager (SM)*** svolga periodicamente un'analisi dei rischi che tenga in considerazione gli obiettivi strategici espressi nella presente Politica, degli incidenti eventualmente occorsi e dei cambiamenti strategici, di business e tecnologici avvenuti.

L'analisi dei rischi ha lo scopo di valutare il rischio associato ad ogni asset da proteggere rispetto alle minacce individuate. La Direzione condivide con il Responsabile della Sicurezza delle informazioni la metodologia da impiegare per la valutazione del rischio, approvando il relativo documento; nella relazione della metodologia, la Direzione partecipa anche alla definizione delle scale di valore da impiegare per valorizzare i parametri che concorrono alla valutazione del rischio.

In seguito alla elaborazione dell'analisi dei rischi, la Direzione valuta i risultati ottenuti accettando la soglia di rischio accettabile, il trattamento di mitigazione dei rischi oltre tale soglia e il rischio residuo in seguito al trattamento.

Tale analisi sarà ponderata anche rispetto al valore di business dei singoli beni da proteggere e dovrà identificare chiaramente le azioni da intraprendere, classificate secondo una scala di priorità che rispetti gli obiettivi aziendali, il budget a disposizione e la necessità di mantenere la conformità alle norme e alle leggi vigenti. Detta analisi dovrà essere effettuata anche a fronte di eventi che possano modificare il profilo di rischio complessivo del sistema.

5. Responsabilità

Tutto il personale che, a qualsiasi titolo, collabora con l'azienda è responsabile dell'osservanza di questa policy e della segnalazione di anomalie, anche non formalmente codificate, di cui dovesse venire a conoscenza.

Security Manager (SM): si occupa della progettazione del *Sistema di Gestione integrato per la Qualità e per la Sicurezza delle informazioni* e, in particolare di:

- emanare tutte le procedure necessarie, ivi inclusa la tipologia di classificazione dei documenti affinché l'organizzazione aziendale possa condurre, in modo sicuro, le proprie attività; ● adottare criteri e metodologie per l'analisi e la gestione del rischio;
- suggerire le misure di sicurezza organizzative, procedurali e tecnologiche a tutela della sicurezza e continuità delle attività di Madisoft S.p.A.;
- pianificare un percorso formativo, specifico e periodico in materia di sicurezza delle informazioni per il personale;
- controllare periodicamente l'esposizione dei servizi aziendali alle principali minacce;
- verificare gli incidenti di sicurezza e adottare le opportune contromisure;
- promuovere la cultura relativa alla sicurezza delle informazioni.

Gli organi di amministrazione e direttivi di Madisoft approvano le misure di gestione del rischio e sovrintendono alla loro attuazione, ai sensi dell'Art. 24 D.Lgs. 138/2024. Questa responsabilità è non delegabile.

Security Champion: figura di riferimento per la sicurezza all'interno dei team di sviluppo, responsabile della promozione delle pratiche di sviluppo sicuro.

Tutti i soggetti esterni, che intrattengono rapporti con Madisoft S.p.A., devono garantire il rispetto dei requisiti di sicurezza delle informazioni esplicitati nella presente Politica, anche attraverso la sottoscrizione di un "**Patto per la Riservatezza**" (***NDA***) all'atto del conferimento del conferimento d'incarico (quando questo tipo di vincolo non sia espressamente citato negli accordi).

6. Aree di Presidio

Sicurezza della catena di fornitura (Art. 21.2.d NIS2): Impegno a monitorare e qualificare i fornitori critici.

Business Continuity e Disaster Recovery (Art. 21.2.c NIS2): Piano di resilienza per garantire la continuità dei servizi.

Gestione degli incidenti (Art. 21.2.b NIS2): Procedure per la rilevazione, risposta e notifica obbligatoria al CSIRT Italia.

Formazione e sensibilizzazione (Art. 21.2.g NIS2): Programmi periodici per tutto il personale.

Controllo accessi e gestione identità: Implementazione di criteri di gestione sicura delle

identità. **Sviluppo sicuro:** Integrazione di metodologie di sviluppo sicuro nel ciclo di vita del

software.

7. Matrice RACI

Ruolo	**Responsabilità (RACI: R=Responsabile operativo, A=Accountable/Approva, C=Consultato, I=Informato)**
Direzione Generale	A (Approva policy, supervisiona - Art. 24 D.Lgs. 138/2024)
Security Manager	R (Responsabile operativo SGI, audit)
IT Manager	R (Implementazione tecnica)
CISO di Gruppo	C (Indirizzo strategico)

Security Champion I (Riferimento sicurezza sviluppo)

HR	I (Onboarding/offboarding compliance, formazione)
DPO	C (Supervisione trattamenti)

8. Cloud computing

Per l'implementazione ed erogazione dei servizi in cloud, ai sensi della **ISO/IEC 27017:2021** e della **ISO/IEC 27018:2020** e del **Regolamento (UE) 2016/679**, la Direzione si impegna ad adottare requisiti di sicurezza e di conformità normativa per garantire anche:

- la protezione dei dati personali degli interessati e che prendano in considerazione i rischi derivanti dal personale interno;
- la gestione sicura del multi-tenancy (condivisione dell'infrastruttura);

- l’accesso agli asset in cloud dei clienti da parte del personale del service provider; -
il controllo degli accessi (in particolare degli amministratori);
- le comunicazioni ai clienti in occasione di cambiamenti dell’infrastruttura;
- la sicurezza dei sistemi di virtualizzazione;
- la protezione e l’accesso dei dati dei clienti in ambiente cloud;
- la gestione del ciclo di vita degli account cloud dei clienti;
- la comunicazione dei data breach;
- le linee guida per la condivisione delle informazioni a supporto delle attività;
- la costante sicurezza sull’ubicazione fisica dei dati nei server in cloud.

Con riferimento ai propri clienti Madisoft S.p.A., ai sensi della **ISO/IEC 27018:2020** e in accordo con **Regolamento (UE) 2016/679**, agisce come Titolare ovvero come Responsabile del Trattamento, dichiarando il rispettivo status e i relativi obblighi che ne discendono nei contratti sottoscritti e nelle nomine a responsabile che Madisoft S.p.A. prevede con i propri fornitori per lo svolgimento delle attività di trattamento.

A tal fine Madisoft S.p.A. pone cura ed attenzione:

- alla corretta identificazione degli interessati dei dati personali che tratta;
- all’esattezza dei dati personali di cui viene in possesso;
- alla liceità dei trattamenti che esegue su tali dati;
- alla ponderata identificazione, valutazione e gestione di tutti i rischi connessi con i diversi trattamenti eseguiti, con eventuale esecuzione di valutazioni di impatto (DPIA), qualora fosse necessario;
- all’adozione di misure tecniche e organizzative adeguate (processi, strumenti e controlli idonei) per garantire, ed essere in grado di dimostrare, che ogni trattamento è effettuato conformemente alla normativa vigente in materia di protezione dei dati personali;
- all’adozione di criteri e metodi di “privacy by design” e “privacy by default” per la piena conformità ai dettami normativi;

- all’identificazione delle responsabilità e autorità coinvolte nella gestione dei dati personali trattati anche afferenti alle nomine pertinenti di DPO (Data Protection Officer), Delegati e Autorizzati al trattamento, Amministratori di Sistema, Responsabili del trattamento.

9. Riesame

Madisoft S.p.A. verificherà periodicamente l’efficacia e l’efficienza *del Sistema di Gestione Integrato Qualità e Sicurezza delle Informazioni*, garantendo l’adeguato supporto per l’adozione delle necessarie migliorie al fine di consentire l’attivazione di un processo continuo che controlli il variare delle condizioni o degli obiettivi di business aziendali al fine di garantire il suo corretto adeguamento.

10. Eccezioni

Ogni deroga alla presente politica deve essere richiesta formalmente al Security Manager, approvata dalla Direzione, documentata e sottoposta a revisione periodica.

11. Governance e Applicazione

La violazione della policy comporta l'applicazione di provvedimenti disciplinari previsti dal CCNL vigente e può determinare conseguenze contrattuali per i fornitori esterni.

12. Documentazione di riferimento

Codice	Titolo	Rev.	Data
DYB.GOV.PO.01	Politica per la Qualità e la Sicurezza delle Informazioni	1	29/04/2026

Il presente documento è redatto in piena coerenza con le Direttive di Sicurezza definite a livello di Gruppo, integrandone i principi cardine all'interno del perimetro operativo, legale e strutturale di Madisoft S.p.A.

L'integrazione progressiva degli ulteriori elementi del framework di Gruppo è stabilita nel piano di perfezionamento costante del SGI, nel pieno rispetto del criterio di proporzionalità delle strategie di difesa indicato dall'Art. 21.1 della **Direttiva (UE) 2022/2555** e dal punto 10.1 della norma **ISO/IEC 27001:2022**.

13. Glossario

SGI: Sistema di Gestione Integrato.

ISMS: Information Security Management System.

NIS2: Network and Information Security Directive 2.

CSIRT: Computer Security Incident Response Team.

RACI: Responsible, Accountable, Consulted, Informed.

DYB: Dylog Buffetti.

BCP: Business Continuity Plan.

DRP: Disaster Recovery Plan.

VAPT: Vulnerability Assessment and Penetration Testing.

DAST: Dynamic Application Security Testing.

SOC: Security Operations Center.

XDR: Extended Detection and Response.

IAM: Identity and Access Management.

RBAC: Role-Based Access Control.

Pollenza (MC) - 29/06/2026

La Direzione

_____