MQI_5.2.A1
POLITICA INTEGRATA DEI SISTEMI DI GESTIONE

Società del Gruppo GMH

MILLENNIUM S.p.A. Direzione e coordinamento GMH S.r.l.
Sede legale: Via di Collodi, 6/C, 50141 Firenze – Tel.055 45544.1 / Fax 0554554.420
Call Center 800 949 502 – www.millewin.it
Commerciale.millennium@dedalus.eu – PEC: millenniumfirenze@legalmail.it
Cap. Soc. € 3.840.000 i.v. – R.E.A Firenze 558973
Registro Imprese Firenze – Codice Fiscale e Partita IVA 05588740489

UNI EN ISO 9001:2015

Tabella delle revisioni

Nr Rev.	Data	Descrizione modifiche	Verificato da:		Approvato da:	Emesso da:
2	28/10/2024	Aggiornamento Politica per adeguamento contenuti a ISO 27001	(OM) Paola Di Marcello	RSGI (Alessandra Rollo)	AD (Giorgio Moretti)	RSGI (Alessandra Rollo)
1	07/02/2023	Aggiornamento Politica per approvazione dalla Direzione	RGQ (Antonio Loguercio)	RDDM (Alessandra Rollo)	AD (Giorgio Moretti)	07/02/2023 RGQ (Antonio Loguercio)
0	12/02/2021	Prima emissione a seguito della revisione generale del sistema qualità Millennium per integrarlo e renderlo conforme ai requisiti ISO 13485	RGQ (Simone Franzolin)	RDDM (Alessandra Rollo)	DIR (Antonello Guggino)	15/02/2021RGQ (Simone Franzolin)

Sommario

1. GENERALITÀ SULLA POLITICA INTEGRATA

1.1 Obiettivo di Millennium

Millennium SpA sviluppa soluzioni per il settore delle Cure Primarie e della Medicina Generale. Riveste un ruolo di fondamentale competenza nell'area dell'integrazione Regionale e Aziendale ed è attiva in tutte le Regioni che hanno avviato progetti di interoperabilità e cooperazione tra i diversi soggetti sanitari quali Medici di Medicina Generale, ASL e Regioni.
La mission aziendale è improntata al superamento della "frammentazione" esistente sul mercato, qualificando l'Azienda come punto di riferimento con importanti capacità di investimento in ricerca e sviluppo.
L'obiettivo di Millennium è quindi di consolidare il proprio ruolo di player primario nel mercato nazionale dei prodotti software per i medici di medicina generale.

1.2 Contenuti e parti costituenti della Politica Integrata dei Sistemi di Gestione di Millennium

A tale scopo la Direzione di Millennium ha definito la Politica Integrata per la Qualità dell'azienda, che comprende gli elementi ritenuti strategici e quindi fondamentali relativamente ai seguenti sistemi di gestione:

- Sistema di Gestione per la Qualità (SGQ), per la conformità alla norma ISO 9001
- Sistema di Gestione della Qualità dei Dispositivi Medici (SGDM), per la conformità alla norma ISO 13485

Sistema di Gestione della Sicurezza delle Informazioni (SGSI), per la conformità alla norma ISO/IEC 27001 e alle relative estensioni ISO/IEC 27017 e ISO/IEC 27018

1.3 Caratteristiche della Politica Integrata dei Sistemi di Gestione

La Direzione assicura che tale politica:

- sia appropriata alle finalità e al contesto dell'organizzazione nonché alle finalità del fornitore del servizio;
- costituisca un quadro di riferimento per fissare gli obiettivi dei sistemi di gestione;
- comprenda un impegno a soddisfare i requisiti applicabili di tutti i sistemi di gestione e a migliorare in modo continuo l'efficacia dei sistemi di gestione;
- comprende l'impegno ad essere **conforme con le leggi nazionali**, le altre leggi applicabili e gli altri requisiti sottoscritti;
- sia disponibile come informazione documentata;
- sia comunicata, compresa e applicata all'interno dell'organizzazione;
- sia disponibile alle parti interessate rilevanti;
- sia riesaminata per accertarne la continua idoneità.

2. POLITICA PER LA GESTIONE DELLA QUALITÀ GENERALE E DEI DISPOSITIVI MEDICI

2.1 Standard applicabili alla sezione

Questa sezione della politica integrata dei sistemi di gestione è riferita in particolare ai requisiti delle norme **ISO 9001** ed **ISO 13485**.

2.2 Principi applicabili

La Direzione di Millennium, convinta dei miglioramenti interni e verso i clienti conseguenti all'adozione di un sistema qualità ha definito la propria politica della qualità, basata sui seguenti principi:

- garantire e migliorare costantemente la soddisfazione dei clienti soddisfacendone le attese ed ottemperando ai requisiti del prodotto e del servizio allo scopo di divenire per loro un partner sempre più importante;
- garantire che i clienti ricevano valore reale attraverso l'erogazione dei propri servizi mediante la definizione ed il rispetto delle SLA;
- favorire il miglioramento continuo della qualità dei prodotti, del servizio, dell'efficacia del sistema qualità;
- rispondere prontamente all'evolvere del mercato mediante una organizzazione flessibile e competitiva;
- raggiungere e mantenere la conformità dei propri dispositivi medici ai requisiti regolatori dei Paesi in cui vengono immessi in commercio;

coinvolgere nei propri processi tutto il personale, consentendogli di crescere professionalmente e di sentirsi parte attiva del sistema qualità.

2.3 Azioni sviluppate

L'attuazione di questa politica ha comportato l'attivazione delle seguenti azioni:

- definire e precisare le responsabilità, i ruoli, i compiti per le diverse fasi dei processi;
- mettere a punto le regole interne assunte come standard di riferimento organizzativo, procedurale ed operativo nella gestione delle attività;
- prevenire il verificarsi di non conformità durante lo svolgimento dei processi;
- identificare e registrare le non conformità, promuovendo l'attivazione di idonee azioni correttive e il consolidamento delle soluzioni adottate;
- promuovere lo sviluppo delle competenze delle risorse professionali, favorendo l'integrazione e la collaborazione tra le aree organizzative interne ed attivando azioni di formazione permanente;
- valorizzare il know-how posseduto, attivando la diffusione delle buone prassi e perseguendone l'ottimizzazione per rendere patrimonio comune metodi di lavoro ed esperienze acquisite;
- assicurare la promozione della focalizzazione sul cliente nell'ambito dell'intera organizzazione, oltre che l'integrità del sistema di gestione stesso.

La Direzione Millennium ha stabilito appropriati processi di comunicazione interna quali ad esempio tramite il sito aziendale in area riservata, e-mail, newsletter, video conferenze e riunioni/incontri infra-sedi.

Per la comunicazione esterna si utilizzano sostanzialmente i seguenti strumenti: advertising, produzione di documentazione aziendale, sito internet e social media, organizzazione eventi e attività di ufficio stampa.

3. POLITICA PER LA GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI ESTESA AL CLOUD COMPUTING

3.1 Standard applicabili alla sezione

Questa sezione della politica integrata dei sistemi di gestione è riferita in particolare ai requisiti della norma
- ISO/IEC 27001

incluse le estensioni alle linee guida:
- **ISO/IEC 27017** per il cloud computing e
- **ISO/IEC 27018** per la gestione delle informazioni personali nei cloud pubblici gestiti da responsabili del trattamento dei dati.

3.2 Principi applicabili

Il Sistema di Gestione della Sicurezza delle Informazioni (SGSI), attribuisce importanza strategica al trattamento delle informazioni stesse, per concretizzare la volontà di garantire la riservatezza, l'integrità e la disponibilità dei dati (il cosiddetto paradigma "RID"), in accordo ai principi della ISO/IEC 27001; i principi cardine del SGSI sono dunque i seguenti:
- la **riservatezza** del patrimonio informativo gestito, per cui l'informazione non è resa disponibile o comunicata ad individui e/o entità non autorizzati;
- l'**integrità** del patrimonio informativo gestito, e cioè che i dati e le informazioni siano protetti da modifiche non autorizzate;
- la **disponibilità** del patrimonio informativo gestito, per cui l'informazione deve essere accessibile e utilizzabile quando necessario (pur sempre rispondendo al criterio della riservatezza indicato in precedenza);
- l'**ottemperanza** ai requisiti cogenti, normativi e contrattuali, con particolare riferimento agli aspetti previsti dal **GDPR** (Regolamento UE 2016/679), al D. Lgs. 196/2003 modificato dal D. Lgs. 101/2018 e a tutta la normativa privacy applicabile ai mercati di riferimento, trattando Millennium anche dati "particolari", così come definiti dal GDPR; tale principio va inteso anche come supporto e impegno di Millennium a raggiungere la compliance con la legislazione di protezione delle informazioni personali e ai requisiti contrattuali concordati tra Millennium che opera come responsabile del trattamento dei dati e i suoi clienti;
- la redazione di piani per la **continuità operativa dei processi** rilevanti per il business e per la gestione del patrimonio informativo dell'organizzazione, e che tali piani siano il più possibile tenuti aggiornati e controllati;
- l'adeguata **formazione del personale** in tema di sicurezza delle informazioni e della normativa privacy applicabile;
- la **corretta gestione di tutte le violazioni** alla sicurezza delle informazioni e dei possibili punti deboli, al fine di una corretta rilevazione ed indagine, con conseguente miglioramento del Sistema.

3.3 Azioni sviluppate

Per garantire l'applicazione concreta di tali principi cardine, Millennium ha definito e mantiene aggiornati nel tempo degli **obiettivi per la sicurezza** delle informazioni, con le modalità previste dal Sistema di Gestione.
Millennium ha definito i criteri di **valutazione dei rischi della sicurezza** delle informazioni considerando in particolare il valore strategico che ha per l'organizzazione l'applicazione del SGSI, le aspettative e le percezioni delle parti interessate (stakeholders) e i possibili danni all'immagine che potrebbero conseguire da una non corretta gestione di tale importante ambito.
Millennium ha definito e documentato una procedura per la comunicazione tempestiva e per la **gestione degli incidenti della sicurezza dell'informazione**, in particolar modo quando questi coinvolgano dati personali (**Data Breach**) con una chiara indicazione dei ruoli e delle azioni correttive da intraprendere.
Millennium è conscia che la sicurezza delle informazioni, non consiste semplicemente in un prodotto/sistema tecnologico da acquistare, ma è un **processo culturale complesso**, che deve coinvolgere tutte le risorse umane ed organizzative aziendali.
Per tale ragione la Direzione si impegna a soddisfare continuativamente i requisiti applicabili e attinenti alla sicurezza delle informazioni secondo la norma ISO/IEC 27001 e a garantire il **miglioramento continuo** del sistema di gestione per la sicurezza delle informazioni stesse.

3.4 Politica della sicurezza delle informazioni per il cloud

La politica della sicurezza delle informazioni di Millennium include sia la gestione che l'utilizzo di servizi cloud in modalità SaaS, IaaS e PaaS per erogare servizi ai propri clienti servizi di alta qualità, affidabilità e sicurezza, nel rispetto dei requisiti normativi e degli standard richiesti dal mercato, dalla normativa e dai contratti stipulati. Nel contesto di tali servizi cloud, **quando Millennium opera come service provider per i propri clienti** ha definito e mantiene sotto controllo:

- le modalità di erogazione dei propri servizi cloud (anche in modalità SaaS), inclusi i relativi SLA anche in termini di disponibilità degli stessi;
- la gestione degli accessi ai servizi erogati in modalità cloud, secondo una politica concordata con il cliente per la gestione degli accessi;
- le comunicazioni ai clienti in caso di change e a clienti, alle autorità e agli interessati, in caso di data breach;
- il ciclo di vita degli account relativi ai servizi cloud e le relative modalità di gestione da parte degli amministratori di sistema coinvolti;
- l'esecuzione dell'analisi dei rischi collegata all'erogazione dei servizi cloud;
- l'applicazione dei requisiti cogenti derivati dal Regolamento Europeo per la Protezione dei Dati Personali (GDPR), considerando le specificità degli ambienti cloud.

Nell'utilizzo di servizi erogati da fornitori di servizi cloud (in particolare anche in modalità IaaS e Paas che possono essere inglobati nei propri servizi), Millennium ha definito e mantiene sotto controllo, tra i vari elementi:

- i requisiti, inclusi quelli relativi alla sicurezza delle informazioni, dei servizi erogati dai servizi cloud provider utilizzati (anche in modalità IaaS e PaaS) per garantire che siano in linea con i requisiti propri, quelli cogenti, quelli richiesti dai propri accreditamenti e quelli contrattuali stabiliti con i clienti;
- gli accordi contrattuali relativi ai servizi cloud per garantire che siano redatti definendo chiaramente le responsabilità sul trattamento dei dati nel cloud, inclusi gli eventuali sub-appaltatori

- le modalità di conservazione e accesso alle informazioni in cloud da parte dei cloud service provider;
- le modalità di mantenimento degli eventuali ambienti multi-tenant in cloud, al fine di garantire sempre un adeguato livello di protezione e segregazione dei dati in relazione ai requisiti contrattuali pattuiti e all'analisi dei rischi dei servizi cloud effettuata;
- il ciclo di vita e le modalità di gestione degli utenti che fruiscono dei servizi cloud ed il contesto in cui li usano;
- l'individuazione e la gestione degli utenti amministratori dei servizi cloud fruiti in modalità customer, dotati di accessi privilegiati;
- la localizzazione geografica dei provider di servizi cloud e i paesi in cui il provider può conservare i dati personali e riservati, anche temporaneamente, per consentire una adeguata gestione dei vincoli legislativi e contrattuali operanti sugli stessi.

Questa politica si applica anche al caso in cui **Millennium operi come Responsabile del trattamento di dati personali nei cloud pubblici** (anche in modalità SaaS o IaaS o PaaS), in relazione ai quali si precisa che il sopra citato principio di **ottemperanza** ai requisiti cogenti, normativi e contrattuali, va inteso anche come supporto e impegno di Millennium a raggiungere la compliance con la legislazione di protezione delle informazioni personali e ai requisiti contrattuali concordati tra Millennium che opera come responsabile del trattamento dei dati e i suoi clienti, secondo quanto previsto dalla ISO / IEC 27018.

4 I PRINCIPI GENERALI A CUI CI ISPIRIAMO

Siamo convinti che per ottenere Qualità ognuno di noi debba portare con sé quotidianamente i seguenti principi:

- bisogna agire con determinazione, perché la qualità e la soddisfazione del cliente si ottengono solo attraverso azioni concrete, con un costante impegno e un profondo senso di responsabilità da parte di ognuno di noi;
- bisogna fare bene le cose fin dalla prima volta, con l'obiettivo di rispettare i requisiti di prodotto e di servizio;
- bisogna essere tempestivi nel rispondere agli eventuali incidenti e reagire con la volontà di eliminare i problemi sottostanti;
- bisogna agire attuando una'attenta e continua prevenzione, così come facciamo quando sono in gioco i nostri interessi personali;
- bisogna pensare a tutti i riflessi che le nostre azioni o le nostre decisioni hanno sulla struttura aziendale, preoccupandoci così di attuare una tempestiva e completa comunicazione a tutti i soggetti interessati il cui intervento seguirà al nostro nel processo organizzativo e/o produttivo che si sta espletando;
- bisogna considerare "Clienti" tutti coloro che ricevono i nostri servizi e/o i nostri prodotti; sono quindi Clienti gli utilizzatori finali, ma anche i nostri colleghi, gli altri reparti dell'Azienda e i Collaboratori esterni, quando l'organizzazione del lavoro preveda che da parte nostra debba essere consegnato a loro un prodotto od erogato un servizio propedeutico al conseguimento del risultato finale, garantendo anche in tal caso conformità alle specifiche pattuite con il "Cliente" stesso; siamo infatti consapevoli che sarà molto improbabile conseguire la Qualità del Servizio alla fine del processo produttivo se non si sono attuate in Qualità una o più delle lavorazioni intermedie;

- bisogna avere la consapevolezza che la scarsa aderenza alle specifiche di Servizio originano un costo elevato per l'Azienda, in termini di necessità di cambiamento dei prodotti, di nuova erogazione dei servizi e in termini di perdita di immagine aziendale.

Riteniamo poi che il vantaggio competitivo sia sempre più generato dal capitale intellettuale e dall'organizzazione aziendale. Crediamo che le menti più interessanti siano quelle che sanno liberare la fantasia, porsi domande inedite, affrontare le sfide e tracciare la strada per chi segue.
Crediamo che un'organizzazione aziendale di successo debba essere basata sulla passione delle proprie persone e imperniata su di un'efficace e continuativa comunicazione interna, sull'orientamento alla soluzione dei problemi, sull'obiettivo di originare la soddisfazione del Cliente: a favore di quest'ultimo, insomma, vogliamo essere un partner a tutto campo e non un semplice Fornitore.

Firenze, 28/10/2024

L'AD
Giorgio Moretti