POLITICA GENERALE PER LA CYBERSICUREZZA

(Dichiarazione pubblica di impegno di MIR - MEDICAL INTERNATIONAL RESEARCH S.P.A. in materia di sicurezza informatica)

La riproduzione del presente documento è vietata senza la preventiva autorizzazione di MIR - MEDICAL INTERNATIONAL RESEARCH S.P.A.

Tabella di revisione:

Controllo del documento	
Autore	Armando Iovino - Progetto Qualità e Ambiente S.r.l.
Proprietà	MIR - MEDICAL INTERNATIONAL RESEARCH S.P.A.
Data di creazione	12/10/2026

Versione	Data approvazione	Approvato da	Descrizione delle modifiche
00	28/10/2026	Consiglio di Amministrazione	Prima emissione

La riproduzione del presente documento è vietata senza la preventiva autorizzazione di MIR - MEDICAL INTERNATIONAL RESEARCH S.P.A.

Sommario:

Aggiornare il sommario aprendo il documento in Word (F9 o tasto destro, Aggiorna campo).

La riproduzione del presente documento è vietata senza la preventiva autorizzazione di MIR - MEDICAL INTERNATIONAL RESEARCH S.P.A.

1. LETTERA DEL CONSIGLIO DI AMMINISTRAZIONE

I dispositivi medici che progettiamo e produciamo accompagnano ogni giorno il lavoro di medici, ospedali e pazienti in molti Paesi. Per farlo bene abbiamo bisogno di sistemi informatici affidabili: per progettare il firmware e il software dei dispositivi, per produrli e collaudarli, per seguirne la qualità e la tracciabilità, per assistere chi li usa. La sicurezza di questi sistemi è quindi parte della qualità dei nostri prodotti, e come tale la trattiamo.

Il Consiglio di Amministrazione ha approvato il sistema con cui MIR governa la sicurezza informatica: le regole, le responsabilità, la valutazione dei rischi e i piani per prevenire, affrontare e superare un incidente. Ne risponde per legge, ne segue l'attuazione e ne riceve conto almeno una volta l'anno. Non è un adempimento delegato agli specialisti: è una responsabilità della Direzione, che si impegna a dare a questo lavoro le persone, il tempo e le risorse che servono.

Con questo documento vogliamo dire con chiarezza a clienti, distributori, fornitori, partner, dipendenti e autorità che cosa facciamo e che cosa ci impegniamo a fare. Abbiamo scelto di scrivere soltanto ciò che è vero oggi o che abbiamo deciso con un piano approvato: la fiducia si costruisce mantenendo gli impegni, non moltiplicandoli.

Il Presidente del Consiglio di Amministrazione

L'Amministratore Delegato

2. CHI SIAMO E PERCHÉ LA CYBERSICUREZZA CI RIGUARDA

MIR - MEDICAL INTERNATIONAL RESEARCH S.P.A. (di seguito «MIR») ha sede a Roma. Progetta, produce e commercializza dispositivi medici per la diagnostica respiratoria: spirometri, sensori di flusso e dispositivi diagnostici a proprio marchio, insieme al firmware e al software che li fanno funzionare, sviluppati in gran parte internamente. Opera con un sistema di gestione per la qualità certificato secondo le norme ISO 9001 e ISO 13485.

La fabbricazione di dispositivi medici è uno dei settori che la direttiva europea NIS 2 sulla sicurezza delle reti e dei sistemi informativi considera importanti per la vita economica e sociale. Per questo MIR è stata inserita dall'Agenzia per la Cybersicurezza Nazionale (ACN) nell'elenco dei soggetti a cui si applica il decreto legislativo 4 settembre 2024, n. 138, che recepisce la direttiva in Italia, con la qualifica di soggetto importante.

La nostra attività dipende dai sistemi informatici in tutte le sue fasi: la ricerca e lo sviluppo, la produzione e il collaudo, la qualità e la documentazione regolatoria, la logistica, l'amministrazione, l'assistenza tecnica e i servizi web per utenti e distributori. Un attacco o un guasto grave potrebbe rallentare la produzione, ritardare le consegne, compromettere la documentazione dei dispositivi o esporre dati di clienti e utenti. Proteggere i sistemi significa proteggere la continuità del servizio, il know-how dell'azienda e la fiducia di chi usa i nostri prodotti.

La riproduzione del presente documento è vietata senza la preventiva autorizzazione di MIR - MEDICAL INTERNATIONAL RESEARCH S.P.A.

3. I NOSTRI PRINCIPI

Il nostro modo di affrontare la sicurezza informatica si fonda su sei principi.

Principio	Che cosa significa per noi
Proporzionalità al rischio	Le misure si scelgono in base ai rischi valutati: si comincia dai sistemi e dai processi il cui fermo o la cui compromissione avrebbe le conseguenze più gravi.
Difesa su più livelli	Nessuna misura basta da sola. Regole di accesso, protezione dei dispositivi, copie di sicurezza, controllo degli eventi e preparazione agli incidenti si sommano, perché il cedimento di una difesa non lasci scoperto il resto.
Responsabilità chiare	Ogni attività di sicurezza ha una funzione che la svolge e una che ne risponde. Le decisioni che contano, come l'accettazione di un rischio, spettano al Consiglio di Amministrazione.
Responsabilità condivisa	La sicurezza riguarda tutti: chi usa i sistemi, chi li gestisce, chi li fornisce. Ognuno riceve le istruzioni e la formazione per fare la propria parte.
Miglioramento continuo	Valutiamo, misuriamo e correggiamo. Le regole si riesaminano almeno una volta l'anno, gli incidenti e le prove diventano lezioni apprese, le difformità diventano azioni con un responsabile e una scadenza.
Trasparenza e conformità	Rispettiamo gli obblighi di legge e comunichiamo in modo tempestivo e corretto con le autorità e con chi è interessato da un incidente.

4. COME CI SIAMO ORGANIZZATI

4.1 Governo e figure di riferimento

Al vertice dell'organizzazione per la sicurezza c'è il Consiglio di Amministrazione. Le figure previste dalla normativa e quelle che MIR ha scelto di affiancare sono indicate qui per ruolo; le persone che le ricoprono sono designate formalmente e comunicate all'ACN nei casi previsti.

Figura	Ruolo
Consiglio di Amministrazione	Approva le politiche, la valutazione del rischio e i piani; sovrintende alla loro attuazione; decide le risorse; è il solo che può accettare un rischio residuo; segue una formazione specifica in materia di sicurezza informatica.
Punto di Contatto NIS	È il Responsabile IT. Tiene i rapporti con l'ACN, cura gli adempimenti previsti dalla legge e informa senza ritardo il Consiglio sugli incidenti significativi.
Responsabile per la sicurezza informatica	Coordina la gestione dei rischi e la risposta agli incidenti, verifica che le misure siano applicate e riferisce al Consiglio almeno una volta l'anno.

La riproduzione del presente documento è vietata senza la preventiva autorizzazione di MIR - MEDICAL INTERNATIONAL RESEARCH S.P.A.

Figura	Ruolo
Referente CSIRT	Trasmette al CSIRT Italia, la struttura nazionale di risposta agli incidenti informatici, le notifiche degli incidenti significativi.
Responsabile IT	Gestisce i sistemi informatici e attua le misure tecniche, direttamente o tramite fornitori specializzati.
Referente Privacy	Raccorda la sicurezza informatica con la protezione dei dati personali, comprese le eventuali notifiche al Garante per la protezione dei dati personali.
Responsabile Qualità e audit interno	Inserisce la sicurezza informatica negli audit interni e segue le azioni di miglioramento, in coordinamento con il sistema qualità.
Responsabili delle Risorse Umane e degli Acquisti	Applicano le regole di sicurezza nella gestione del personale, nella formazione e nei rapporti con i fornitori.

La verifica dell'applicazione delle misure è tenuta distinta dalla loro esecuzione: chi gestisce un sistema non è anche l'unico a controllarlo.

4.2 Il sistema documentale

Le regole di sicurezza di MIR sono raccolte in un sistema documentale organizzato su tre livelli:

- un Modello Organizzativo, che descrive l'insieme del sistema, i ruoli, i documenti e il loro regime di approvazione;
- sedici politiche di sicurezza informatica, una per ciascun ambito: gestione del rischio, ruoli e responsabilità, risorse umane, conformità e audit, catena di fornitura, beni informatici, vulnerabilità, continuità operativa e gestione delle crisi, identità e accessi, sicurezza fisica, formazione, protezione dei dati, sviluppo e configurazione dei sistemi, reti e comunicazioni, monitoraggio degli eventi, gestione degli incidenti;
- un Manuale delle procedure operative e i piani che le politiche richiedono, accompagnati dai registri che dimostrano l'applicazione delle regole.

Il Modello Organizzativo, le politiche, la valutazione del rischio e i piani principali sono approvati dal Consiglio di Amministrazione. Le politiche sono riesaminate almeno una volta l'anno.

5. LE NOSTRE AREE DI INTERVENTO

Questa sezione descrive in linguaggio semplice come affrontiamo i temi principali della sicurezza informatica. Per ovvie ragioni di sicurezza non riporta dettagli tecnici sui nostri sistemi.

5.1 Gestione del rischio

Valutiamo i rischi per i sistemi da cui dipende la nostra attività combinando la gravità delle conseguenze con la probabilità che l'evento si verifichi. Da questa valutazione nasce un piano di trattamento che indica, per ogni rischio, che cosa si fa, chi lo fa ed entro quando. La valutazione si ripete almeno ogni due anni e ogni volta che cambiano in modo significativo i sistemi o il modo in cui sono gestiti.

La riproduzione del presente documento è vietata senza la preventiva autorizzazione di MIR - MEDICAL INTERNATIONAL RESEARCH S.P.A.

5.2 Protezione degli accessi

Le nostre regole prevedono che ogni persona, compresi gli operatori dei fornitori, acceda ai sistemi con un'utenza personale e con i soli privilegi che servono al suo lavoro. Gli accessi si concedono su autorizzazione, si riesaminano periodicamente e si revocano quando una persona cambia mansione o lascia l'azienda. Le utenze con privilegi di amministrazione sono assegnate a persone designate e tenute distinte da quelle di uso quotidiano. Il nostro piano di adeguamento prevede l'autenticazione a più fattori per gli accessi da remoto, per i servizi in cloud e per le utenze di amministrazione, e un gestore sicuro delle credenziali amministrative.

5.3 Protezione dei sistemi, delle reti e dei dati

Le postazioni di lavoro e i server sono protetti da una soluzione di protezione degli endpoint con rilevamento delle minacce, controllata da una console centrale. La rete aziendale è suddivisa in zone, con una rete separata per gli ospiti. Le nostre regole ammettono soltanto software ancora aggiornato dal produttore, con eccezioni temporanee, motivate e registrate, e fissano i tempi per applicare gli aggiornamenti di sicurezza secondo la gravità delle vulnerabilità che correggono.

I sistemi principali sono ospitati in un data center gestito da un fornitore specializzato, su un'infrastruttura virtualizzata con componenti ridondate. I dati sono protetti da copie di sicurezza regolari, con una copia conservata fuori sede. Le nostre regole prevedono inoltre una copia scollegata dalla rete o non modificabile, la cifratura dei dispositivi portatili e prove di ripristino periodiche: sono impegni del nostro piano di adeguamento, ciascuno con un responsabile e una scadenza.

5.4 Continuità operativa e ripristino

Abbiamo analizzato i processi aziendali critici per stabilire, per ciascuno, per quanto tempo al massimo può restare fermo e in quanto tempo deve ripartire. Su questi tempi, approvati dal Consiglio di Amministrazione, sono costruiti tre piani: un piano di continuità operativa, che dice come si continua a lavorare durante un'interruzione; un piano di ripristino, che dice in quale ordine e come si riattivano i sistemi; un piano di gestione delle crisi, che dice chi decide e come si comunica quando un evento supera la gestione ordinaria.

I sistemi principali sono replicati in un secondo sito, distante dal primo, predisposto per riattivarli in caso di disastro. Un tempo di ripristino per noi è dimostrato solo quando una prova lo ha misurato: per questo i piani prevedono ogni anno una prova completa di ripristino e un'esercitazione sulla gestione di una crisi, e ogni sei mesi una prova di ripristino a campione.

5.5 Gestione delle vulnerabilità e sicurezza dei prodotti

Seguiamo con regolarità gli avvisi del CSIRT Italia e dei produttori dei sistemi che usiamo. Per ogni vulnerabilità che ci riguarda valutiamo la gravità e la risolviamo entro tempi stabiliti, più brevi per le vulnerabilità critiche e per quelle già sfruttate dagli attaccanti. Il nostro piano prevede anche scansioni periodiche dei sistemi.

Per lo sviluppo del firmware e del software dei nostri dispositivi le nostre regole prevedono pratiche di sviluppo sicuro e di gestione controllata delle modifiche. Le segnalazioni di vulnerabilità sui nostri prodotti, da qualunque parte arrivino, sono prese in carico dal responsabile per la sicurezza informatica e, quando riguardano un dispositivo medico, sono valutate anche per i loro

La riproduzione del presente documento è vietata senza la preventiva autorizzazione di MIR - MEDICAL INTERNATIONAL RESEARCH S.P.A.

effetti sulla sicurezza del dispositivo, secondo il nostro sistema qualità e le regole sui dispositivi medici.

5.6 Sicurezza della catena di fornitura

Una parte importante dei nostri servizi informatici è affidata a fornitori. Li classifichiamo in base a quanto sono critici per la sicurezza, chiediamo loro impegni di sicurezza proporzionati e ne verifichiamo il rispetto. Gli accessi dei fornitori ai nostri sistemi devono essere personali, autorizzati e tracciati. I requisiti di sicurezza sono raccolti in un allegato contrattuale, che inseriamo nei contratti di fornitura secondo il nostro piano di adeguamento. Restiamo comunque responsabili dei nostri dati e dei nostri obblighi, anche quando un servizio è gestito da altri.

5.7 Formazione e consapevolezza

La formazione in materia di sicurezza informatica coinvolge tutto il personale, con contenuti più approfonditi per chi ha ruoli tecnici, e i componenti del Consiglio di Amministrazione, come richiede la legge. Chi entra in azienda riceve le istruzioni essenziali quando gli vengono attivate le credenziali di accesso. Il programma è definito in un piano di formazione su due anni, approvato dal Consiglio, e la partecipazione è registrata.

5.8 Risposta agli incidenti

Chiunque noti un evento sospetto lo segnala subito. Un piano di gestione degli incidenti stabilisce come si riconosce un incidente, chi lo coordina, come lo si contiene e come si ripristinano i servizi. Quando un incidente è significativo secondo i criteri dell'ACN lo notifichiamo al CSIRT Italia nei termini di legge: una pre-notifica entro 24 ore da quando ne veniamo a conoscenza, una notifica entro 72 ore e una relazione finale entro un mese. Se sono coinvolti dati personali, valutiamo in parallelo la notifica al Garante per la protezione dei dati personali. Dopo ogni incidente significativo analizziamo che cosa è accaduto e correggiamo ciò che va corretto.

6. I NOSTRI IMPEGNI VERSO GLI STAKEHOLDER

6.1 Verso i clienti, gli utenti e i distributori

- Proteggere i sistemi da cui dipendono la produzione, la qualità e l'assistenza dei dispositivi che forniamo.
- Trattare i dati che ci affidano con le misure di sicurezza adeguate e nel rispetto della normativa sulla protezione dei dati personali.
- Informarli senza ingiustificato ritardo quando un incidente significativo può incidere sui servizi che ricevono, indicando, quando è possibile, le misure che possono adottare.
- Prendere in carico le segnalazioni di vulnerabilità sui nostri prodotti e dare riscontro a chi le invia.

6.2 Verso i fornitori e i partner

- Definire con chiarezza, nei contratti, i requisiti di sicurezza e la ripartizione delle responsabilità.

La riproduzione del presente documento è vietata senza la preventiva autorizzazione di MIR - MEDICAL INTERNATIONAL RESEARCH S.P.A.

- Proteggere le informazioni che ci condividono e limitare i loro accessi ai nostri sistemi a quanto serve per il servizio.
- Collaborare nella gestione degli incidenti che coinvolgono entrambi.

6.3 Verso i dipendenti e i collaboratori

- Fornire strumenti sicuri, regole chiare e la formazione necessaria per applicarle.
- Proteggere i loro dati personali.
- Favorire la segnalazione tempestiva degli eventi sospetti: chi segnala in buona fede un possibile problema di sicurezza fa la cosa giusta.

6.4 Verso le autorità

- Collaborare con l'Agenzia per la Cybersicurezza Nazionale e con il CSIRT Italia, tenere aggiornate le informazioni richieste e notificare gli incidenti significativi nei termini di legge.
- Mettere a disposizione dell'Autorità, se richiesto, la documentazione che dimostra l'adozione delle misure.
- Collaborare con il Garante per la protezione dei dati personali e con le autorità competenti sui dispositivi medici per quanto di loro competenza.

7. CONFORMITÀ NORMATIVA

MIR è un soggetto importante ai sensi del decreto legislativo 4 settembre 2024, n. 138, che recepisce la direttiva (UE) 2022/2555 (direttiva NIS 2), e applica le misure di sicurezza stabilite per i soggetti importanti dalla Determinazione dell'Agenzia per la Cybersicurezza Nazionale n. 379907 del 19 dicembre 2025. Il sistema di sicurezza informatica si integra con il sistema di gestione per la qualità certificato ISO 9001 e ISO 13485 e con gli adempimenti del Regolamento (UE) 2016/679 sulla protezione dei dati personali.

Nel 2026 un audit di conformità, svolto con il supporto di consulenti esterni, ha confrontato le nostre pratiche con i requisiti di legge. Le difformità emerse sono diventate azioni di un piano di adeguamento approvato dal Consiglio di Amministrazione, nel quale ogni azione ha una funzione responsabile e una scadenza. Il termine di legge per l'adozione delle misure è il 31 ottobre 2026; le azioni che richiedono acquisti o interventi più lunghi hanno scadenze fissate dal Consiglio. Lo stato di avanzamento è seguito con regolarità e riferito al Consiglio almeno una volta l'anno.

La presente Politica è riesaminata almeno una volta l'anno, insieme alle politiche di sicurezza informatica, ed è approvata dal Consiglio di Amministrazione.

8. CONTATTI

Per comunicazioni ufficiali in materia di sicurezza informatica:

- posta elettronica certificata (PEC): mirsrl-medicalinternationalresearch@pec.it;
- sito istituzionale: www.spirometry.com.

La riproduzione del presente documento è vietata senza la preventiva autorizzazione di MIR - MEDICAL INTERNATIONAL RESEARCH S.P.A.

8.1 Segnalazione di vulnerabilità

Chi individua una possibile vulnerabilità in un nostro dispositivo, in un nostro software o in un nostro servizio può segnalarla alla posta elettronica certificata indicata sopra, descrivendo il prodotto o il servizio interessato e, se possibile, come riprodurre il problema. Prendiamo in carico ogni segnalazione e diamo riscontro a chi l'ha inviata entro cinque giorni lavorativi dalla ricezione. Chiediamo a chi segnala di darci il tempo di verificare e correggere il problema prima di renderlo pubblico.

8.2 Segnalazioni all'autorità nazionale

Gli incidenti informatici possono essere segnalati al CSIRT Italia, anche su base volontaria, attraverso il portale delle segnalazioni dell'Agenzia per la Cybersicurezza Nazionale: segnalazioni.acn.gov.it.

La riproduzione del presente documento è vietata senza la preventiva autorizzazione di MIR - MEDICAL INTERNATIONAL RESEARCH S.P.A.