Politica Aziendale

TITOLO: Politica del Sistema di Gestione per la Sicurezza delle informazioni (SGSI)

Documento	Ruolo
Redazione	*RSGSI*
Approvazione	*IT Senior Manager*
Classificazione	*PUBLIC*

La presente Politica è predisposta in coerenza con i requisiti normativi, regolamentari e con gli standard applicabili riportati nella tabella seguente.

Norma / Standard	Riferimento
Direttiva (UE) 2022/2555 (NIS2)	*Requisiti in materia di governance della sicurezza informatica, gestione del rischio, continuità operativa e sicurezza della supply chain.*
Decreto Legislativo 4 settembre 2024, n. 138	*Recepimento nazionale della Direttiva NIS2 e definizione degli obblighi per i soggetti essenziali e importanti.*
ISO/IEC 27001	*Requisiti per l'istituzione, l'attuazione, il mantenimento e il miglioramento continuo del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI).*
ISO/IEC 27002	*Linee guida e controlli di sicurezza delle informazioni a supporto dell'ISO/IEC 27001.*
Regolamento (UE) 2016/679 (GDPR)	*Principi e misure per la protezione dei dati personali e la sicurezza del trattamento.*

Indice

1. Scopo

La presente Politica del Sistema di Gestione per la Sicurezza delle Informazioni (di seguito, la "Politica") definisce i principi, gli obiettivi e gli indirizzi strategici adottati da MEMC Electronic Materials S.p.A. (di seguito "MEMC") per garantire la sicurezza delle informazioni, nonché per l'implementazione, il mantenimento e il miglioramento continuo del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI), in conformità alla norma ISO/IEC 27001:2022.

Il campo di applicazione della Politica coincide con il perimetro del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) dell'Organizzazione: *progettazione, implementazione, assistenza e gestione operativa dei sistemi ICT, incluse infrastrutture, applicazioni e servizi di supporto erogati dal Dipartimento IT a sostegno delle attività aziendali e dei processi di produzione di lingotti e fette di silicio monocristallino, per le due sedi italiane di Merano e Novara.*

Rientrano nel perimetro di applicazione l'insieme dei processi, delle attività, dei sistemi informativi e delle infrastrutture tecnologiche e organizzative utilizzate per il perseguimento degli obiettivi aziendali e tutte le informazioni trattate, indipendentemente dalla forma, dal supporto o dalla modalità di trattamento (digitale, cartacea o altra), nonché dal luogo in cui esse sono conservate o trattate.

La presente Politica si applica ed è vincolante per tutti i soggetti che, a qualunque titolo, operano per conto o nell'interesse dell'Organizzazione, inclusi, a titolo esemplificativo e non esaustivo, gli organi di amministrazione e direzione, i dipendenti, i collaboratori, i consulenti, i fornitori, i partner e qualsiasi altro soggetto terzo che abbia accesso alle informazioni o ai sistemi informativi di MEMC.

La presente Politica fornisce inoltre il quadro di riferimento per la definizione, il monitoraggio e il riesame degli obiettivi di sicurezza delle informazioni, in coerenza con il contesto organizzativo, il profilo di rischio e i requisiti applicabili.

2. Principi della politica per la sicurezza delle informazioni

MEMC riconosce la sicurezza delle informazioni quale elemento essenziale per la tutela del proprio patrimonio informativo, per l'affidabilità dei processi aziendali e per la continuità delle attività operative

In tale contesto, l'Organizzazione si impegna a:

- garantire la riservatezza, l'integrità e la disponibilità delle informazioni;
- adottare un approccio basato sul rischio (risk-based) alla gestione della sicurezza delle informazioni, basato sull'identificazione, analisi e trattamento dei rischi in relazione al contesto organizzativo e alle minacce emergenti**;**
- prevenire e ridurre l'impatto di eventi e incidenti che possano compromettere la sicurezza delle informazioni;
- assicurare la continuità dei servizi e dei processi critici;
- migliorare in modo continuo l'efficacia del SGSI, tenendo conto dell'evoluzione del contesto interno ed esterno, delle minacce e delle tecnologie;
- integrare i principi di sicurezza by design e by default nei processi, nei sistemi e nei servizi;

- promuovere la formazione, la consapevolezza e la responsabilizzazione del personale in materia di sicurezza delle informazioni**.**

3. Responsabilità

MEMC ha individuato specifiche figure responsabili della gestione dei rischi per la sicurezza delle informazioni, alle quali sono attribuite responsabilità chiaramente definite in relazione ai rispettivi ambiti di competenza, nonché adeguate interfacce per la gestione dei rapporti con soggetti terzi**,** in coerenza con i requisiti del Sistema di Gestione per la Sicurezza delle Informazioni**.**

In particolare, sono state individuate le figure del Responsabile del Sistema di Gestione per la Sicurezza delle Informazioni (RSGSI) e del Risk Owner, incaricati di:

• assicurare che il Sistema di Gestione per la Sicurezza delle Informazioni sia istituito, attuato, mantenuto e migliorato in conformità alla presente Politica e ai requisiti applicabili, garantendo la disponibilità delle risorse umane, tecnologiche e organizzative necessarie;

• coordinare operativamente il Sistema di Gestione per la Sicurezza delle Informazioni e monitorarne le prestazioni, assicurando la raccolta, l'analisi e la comunicazione delle informazioni rilevanti alla Direzione;

• garantire che le attività svolte nell'ambito del SGSI siano orientate alla tutela della riservatezza, dell'integrità e della disponibilità delle informazioni;

• assicurare la gestione delle non conformità e degli incidenti di sicurezza delle informazioni, incluse le attività di analisi, trattamento, monitoraggio e attuazione delle azioni correttive e preventive previste**,** in coordinamento con le funzioni competenti e in conformità alle procedure di gestione degli incidenti e delle non conformità**;**

• definire e mantenere i criteri e le modalità di comunicazione delle informazioni relative alla sicurezza delle informazioni, individuando le parti interessate interne ed esterne, i soggetti responsabili della comunicazione e le tempistiche di diffusione;

• adottare e attuare i programmi di formazione, addestramento e sensibilizzazione in materia di sicurezza delle informazioni, assicurandone l'applicazione a tutte le persone che rivestono un ruolo all'interno del SGSI

Il personale IT e gli Amministratori di Sistema sono responsabili dell'attuazione tecnica delle misure di sicurezza e della gestione operativa dei sistemi informativi, nel rispetto delle procedure e delle disposizioni organizzative adottate**,** garantendo l'applicazione delle misure di sicurezza definite e il monitoraggio delle attività sui sistemi informativi**.**

L'Alta Direzione è responsabile ultima dell'adozione, dell'approvazione e del riesame della presente Politica e dell'efficacia del Sistema di Gestione per la Sicurezza delle Informazioni.

4. Comunicazione, riesame e aggiornamento

La presente Politica è comunicata a tutto il personale attraverso i canali interni ufficiali e alle altre parti interessate mediante pubblicazione sul sito web dell'Organizzazione.

La Politica è soggetta a riesame periodico e ogniqualvolta si verifichino cambiamenti significativi nel contesto organizzativo, tecnologico o normativo, ovvero a seguito di incidenti di sicurezza o risultanze di audit**,** nonché in relazione all'evoluzione del profilo di rischio dell'Organizzazione**.**

Ogni aggiornamento è approvato dalla Direzione e comunicato tempestivamente alle parti interessate.