

## 1. SCOPO

Lo scopo del presente documento è quello di descrivere i principi generali di sicurezza delle informazioni definiti da ART SpA al fine di sviluppare un efficiente e sicuro Sistema di Gestione della Sicurezza delle informazioni.

I piani strategici di ART S.p.a., il mercato di riferimento e le parti interessate costituiscono il contesto per l'implementazione ed il mantenimento del Sistema di Gestione della Sicurezza delle Informazioni (SGSI).

## 2. DESCRIZIONE

I requisiti per la sicurezza delle informazioni sono coerenti con gli obiettivi dell'Organizzazione, e il Sistema di Gestione della Sicurezza delle Informazioni (di seguito "SGSI") rappresenta lo strumento che consente la condivisione delle informazioni, lo svolgimento di operazioni corrette e la mitigazione dei rischi connessi alle informazioni.

La Sicurezza delle Informazioni per ART SpA ha come obiettivo primario la protezione dei dati e delle informazioni, della struttura tecnologica, fisica e logica, ma anche organizzativa e la loro gestione.

Questo significa costruire e mantenere un sistema di gestione per la Sicurezza delle informazioni (di seguito SGSI) volto a proteggere la *riservatezza*, *l'integrità* e *la disponibilità* delle *informazioni* e degli *asset informativi* individuati nel campo di applicazione al fine di

- garantire la continuità operativa e di business proteggendo il proprio knowhow, valore intangibile di ART Spa;
- preservare il vantaggio competitivo, l'unicità e le peculiarità di ART Spa;
- incrementare la profittabilità e l'affidabilità di ART Spa;
- garantire la conformità legale, regolamentare e contrattuale di ART Spa;
- preservare e rafforzare l'immagine aziendale e del brand di ART Spa nel mercato di riferimento.

Per Riservatezza si intende: assicurare che l'informazione o i dati personali siano accessibili solo a soggetti o a processi autorizzati espressamente.

Per Integrità: la salvaguardia e consistenza delle informazioni da modifiche non autorizzate.

Per Disponibilità. Assicurare che gli utenti autorizzati abbiano accesso alle informazioni e ai dati quando ne fanno richiesta e per tutto il tempo necessario.

## 3. AMBITO DI APPLICAZIONE

La politica per la Sicurezza delle Informazioni si applica a tutto il personale di ART S.p.A. operante nel campo della progettazione, sviluppo e produzione di componenti elettronici ed elettromeccanici per applicazioni dell'infotainment e produzione industriale, alle terze parti che

	<b>Information Security Policy</b>	SGSI.ART.PSGSI.R.00
		Pag. 2 di 3

collaborano alla gestione delle informazioni e a tutti i processi coinvolti nel perimetro stabilito dal Sistema di Gestione delle Informazioni.

Tutti i soggetti coinvolti appartenenti ad ART S.p.a. e gli stakeholders devono assumere comportamenti conformi a quanto indicato in questa Politica e nel Sistema di Gestione della Sicurezza delle Informazioni che la implementa. Tutti gli interessati ricevono, a tal riguardo, la necessaria e opportuna formazione.

#### **4. POLITICA PER LA SICUREZZA DELLE INFORMAZIONI**

La politica della Sicurezza delle Informazioni di ART rappresenta l'impegno di tutta l'organizzazione nei confronti di clienti e terze parti a garantire la sicurezza delle informazioni secondo i seguenti principi:

- a) Garantire all'organizzazione la piena conoscenza delle informazioni gestite e la valutazione della loro criticità, al fine di agevolare l'implementazione degli adeguati livelli di protezione.

La dichiarazione di applicabilità (Statement Of Applicability – SOA), il documento di analisi dei rischi ed il conseguente piano di trattamento, a cura del Responsabile del SGSI, definiscono le modalità attraverso cui realizzare la sicurezza delle informazioni.

- b) Garantire la Sicurezza delle informazioni come elemento essenziale delle reti, dei sistemi informativi, dei processi, delle operazioni e degli accessi alle informazioni, in modo da prevenire trattamenti non autorizzati o realizzati senza i diritti necessari.

La business continuity e i piani di emergenza, le procedure di salvataggio dei dati, la protezione da malware e intrusioni, il controllo degli accessi ai sistemi e i meccanismi di reporting relativi alla sicurezza delle informazioni sono quindi, fondamentali ulteriori del Sistema di gestione, nonché gli Indicatori di controllo supportati da specifiche procedure.

- c) Garantire che l'organizzazione e le terze parti collaborino al trattamento delle informazioni adottando procedure volte al rispetto di adeguati livelli di sicurezza.
- d) Garantire che le anomalie e gli incidenti aventi ripercussione sul sistema informativo e sui livelli di sicurezza siano tempestivamente rilevati, riconosciuti e correttamente gestiti attraverso efficienti sistemi di prevenzione, comunicazione e reazione al fine di minimizzare l'impatto sul business.
- f) Garantire che l'accesso alla sede e ai singoli locali aziendali avvenga esclusivamente da personale autorizzato a garanzia della sicurezza delle aree e degli asset presenti.
- g) Garantire la conformità con i requisiti di legge ed il rispetto degli impegni di sicurezza stabiliti.

La politica della sicurezza delle informazioni è formalizzata nell' ISMS e condivisa con l'organizzazione, le terze parti ed i clienti, attraverso un sistema intranet e specifici canali di comunicazione.



### 5.RESPONSABILITÀ DELLA POLITICA DI SICUREZZA DELLE INFORMAZIONI

La Direzione è responsabile del sistema di gestione per la sicurezza delle informazioni, in coerenza con l'evoluzione del contesto aziendale e di mercato, valutando eventuali azioni da intraprendere a fronte di eventi come:

- evoluzioni significative del business;
- nuove minacce rispetto a quelle considerate nell'attività di analisi del rischio;
- significativi incidenti di sicurezza;
- evoluzione del contesto normativo e legislativo in materia di trattamento delle informazioni;

La presente politica è, pertanto, periodicamente riesaminata al fine di considerare qualsiasi cambiamento nella valutazione dei rischi e, conseguentemente, nel relativo piano di trattamento.

Voc. Pischiello, settembre 2023

CEO



**ART S.p.A.**  
*Il Legale Rappresentante*