	RUOLO	NOME E COGNOME	FIRMA	DATA
Redattore	IT Manager ISMS Manager	Paolo Scotti		01/09/2025
Verificatore	COO & CIO	Jean-Paul David		01/09/2025
Approvatore	CEO	Thibaut Fraisse		01/09/2025

INDICE DELLE REVISIONI	
Rev.	**Motivo della revisione**

CHROMAVIS
FAREVA

ATTIVITÀ DI DIVULGAZIONE	MODALITÀ DI DIFFUSIONE
☑ INFORMAZIONE ☐ FORMAZIONE (in carico al responsabile di reparto/funzione o da QA/HSE) ☐ ADDESTRAMENTO (in carico al responsabile di reparto/funzione o da QA/HSE)	☑ Notifica Sinergest ☐ Notifica portale Zucchetti ☐ Archiviazione presso Quality Info Point ☐ M18_c Registro formazione/addestramento ☐ OPL n° _____ ☐ Scheda incontro Sinergest ☐ Altro:
La comunicazione alle funzioni coinvolte avviene tramite notifica e-mail del sistema Sinergest secondo quanto inserito nella sezione "Gruppi di distribuzione".	

Sommario

1. Scopo

La diffusione delle tecnologie ICT a tutti i livelli della società comporta un aumento dei rischi per la sicurezza in termini di perdita di dati, intrusioni, perdita della riservatezza e violazioni della privacy, e ciò vale in particolare per i sistemi informatici, richiedendo pertanto una accurata analisi delle loro debolezze e delle possibilità di un loro utilizzo non sicuro. L'implementazione di un adeguato sistema di protezione delle informazioni si basa su una sistematica analisi delle possibili minacce, e sulla determinazione delle precauzioni da adottare. La presente politica descrive ad alto livello i princìpi e gli obiettivi che l'azienda ha fatto propri al fine di garantire un sistema di gestione che riduca per quanto possibile i rischi associati alle diverse minacce, e sia strumento di miglioramento continuo.

Su tali basi Chromavis Spa ha deciso di porre in essere un Sistema di Gestione per la Sicurezza delle Informazioni (ISMS) definito secondo regole e criteri previsti dalle "best practice" e dagli standard internazionali di riferimento in conformità alle indicazioni della norma UNI CEI ISO/IEC 27001:2022.

1.1 Contesto applicazione della politica

La politica si applica a tutte le infrastrutture software e hardware, dispositivi, sistemi e dati aziendali, copre tutti i prodotti e servizi aziendali e deve essere rispettata da tutti i dipendenti e fornitori.

1.2 Obiettivo della politica

Il Sistema Informativo (inclusivo delle risorse tecnologiche, hardware, software, informazioni in qualsiasi formato, dati, documenti, reti telematiche e delle risorse umane dedicate alla loro amministrazione, gestione e utilizzo) rappresenta uno strumento di primaria importanza per il conseguimento degli obiettivi strategici e operativi di Chromavis Spa, in considerazione della criticità dei processi aziendali che dipendono da esso. Il presente documento ha l'obiettivo di definire le politiche sui sistemi informativi e la policy sulla sicurezza delle informazioni al fine di sviluppare un efficiente e sicuro Sistema di Gestione della Sicurezza delle Informazioni attraverso il rispetto delle seguenti proprietà:

- Riservatezza: assicurare che l'informazione sia accessibile solamente ai soggetti e/o ai processi debitamente autorizzati
- Integrità: salvaguardare la consistenza dell'informazione da modifiche e cancellazioni non autorizzate
- Disponibilità: assicurare che gli utenti autorizzati abbiano accesso alle informazioni e agli elementi architetturali associati quando ne fanno richiesta
- Controllo: assicurare che la gestione dei dati avvenga sempre attraverso processi e strumenti sicuri e testati
- Autenticità: garantire una provenienza affidabile dell'informazione
- Privacy: garantire la protezione ed il controllo dei dati personali.

L'osservanza dei livelli di sicurezza stabiliti da Chromavis Spa attraverso l'implementazione dell'ISMS, permette di:

• preservare al meglio l'immagine dell'azienda quale fornitore affidabile e competente
• proteggere al meglio il patrimonio informativo proprio e dei propri clienti
• aumentare, nel proprio personale, il livello di sensibilità e la competenza sui temi di sicurezza dei dati
• rispondere pienamente alle indicazioni della normativa vigente e cogente e degli standard internazionali di sicurezza dei dati.

2. Politica sulla sicurezza delle informazioni

La politica della sicurezza di Chromavis Spa rappresenta l'impegno dell'organizzazione nei confronti di clienti e terze parti a garantire la sicurezza delle informazioni, degli strumenti fisici, logici e organizzativi atti al trattamento delle informazioni in tutte le attività.

La politica della sicurezza delle informazioni di Chromavis Spa si ispira ai seguenti principi:

• 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.

• Garantire l'accesso sicuro alle informazioni, in modo da prevenire trattamenti non autorizzati o realizzati senza i diritti necessari.

• Garantire che l'organizzazione e le terze parti collaborino al trattamento delle informazioni adottando procedure volte al rispetto di adeguati livelli di sicurezza.

• Garantire che l'organizzazione e le terze parti che collaborano al trattamento delle informazioni, abbiano piena consapevolezza delle problematiche relative alla sicurezza.

• Garantire che le anomalie e gli incidenti aventi ripercussioni sul sistema informativo e sui livelli di sicurezza aziendale siano tempestivamente riconosciuti e correttamente gestiti attraverso efficienti sistemi di prevenzione, comunicazione e reazione al fine di minimizzare l'impatto sul business.

• Garantire che l'accesso alle sedi ed ai singoli locali aziendali avvenga esclusivamente da personale autorizzato, a garanzia della sicurezza delle aree e degli asset presenti.

• Garantire la conformità con i requisiti di legge ed il rispetto degli impegni di sicurezza stabiliti nei contratti con le terze parti.

• Garantire la rilevazione di eventi anomali, incidenti e vulnerabilità dei sistemi informativi al fine di rispettare la sicurezza e la disponibilità dei servizi e delle informazioni.

• Garantire la business continuity aziendale e il disaster recovery, attraverso l'applicazione di procedure di sicurezza stabilite.

La politica della sicurezza delle informazioni formalizzata nell'ISMS, viene costantemente aggiornata per assicurare il suo continuo miglioramento ed è condivisa con l'organizzazione, le terze parti ed i clienti, attraverso un sistema intranet e specifici canali di comunicazione.

3. Responsabilità della politica

Chromavis Spa ha identificato il modello organizzativo relativo alla gestione della sicurezza delle informazioni riportato nel suo Sistema di Gestione della Sicurezza delle Informazioni (ISMS). Per ogni ruolo, nel contesto dell'Information Security Management System, sono dettagliate le responsabilità e le autorità.

Nell'ambito del Sistema di Gestione della Sicurezza delle Informazioni (ISMS), ogni ruolo aziendale deve essere chiaramente definito in termini di responsabilità e autorità, come richiesto dalla norma ISO27001, par.5.

Gli enti aziendali coinvolti sono:

- Comitato Direttivo
- Chief Information Officer – CIO
- Responsabile Risorse Umane – VP HR
- IT Manager & CISO
- IT Compliance Manager
- Infrastructure Manager
- Application Manager

4. Riesame della politica

La presente Politica Aziendale della Sicurezza sarà revisionata periodicamente sia in caso di eventi esterni, quali ad esempio modifiche della normativa esterna ovvero indicazioni delle Autorità, sia di modifiche organizzative ed operative che abbiano impatto sui Sistemi Informativi e sulla sicurezza delle informazioni.

La presente Politica verrà comunque riconfermata e sottoscritta con cadenza annuale. La sua sottoscrizione avverrà durante l'attività di Riesame della Direzione dell'ISMS.

In particolare, l'aggiornamento della Politica e delle prassi operative è indispensabile laddove in fase di Riesame della Direzione si identifichino:

• Evoluzioni significative del business

• Nuove minacce rispetto a quelle considerate nell'attività di analisi del rischio

• Significativi incidenti di sicurezza

• Nuovi requisiti e pressioni da parte dei mercati di riferimento

• Evoluzione del contesto normativo o legislativo in materia di trattamento sicuro delle informazioni