POL Politica di sicurezza delle informazioni

Nome della società	Aries Srl
Data di entrata in vigore	15/05/2025

Storia della versione

Versione	Data	Descrizione	Autore	Approvato da
1	15/05/2025	-- N / D --	Flavio Marchetto	Flavio Marchetto

Scopo

Lo scopo della presente politica è dichiarare e comunicare l'impegno del Top Management verso la protezione degli asset informativi dell'organizzazione. Questo documento definisce il quadro di riferimento per istituire, attuare, mantenere e migliorare continuamente il Sistema di Gestione della Sicurezza delle Informazioni (SGSI), al fine di proteggere la riservatezza, l'integrità e la disponibilità delle informazioni e di supportare gli obiettivi strategici aziendali.

Indice

Campo di applicazione

La presente politica definisce i principi, gli obiettivi e le responsabilità per la gestione della sicurezza delle informazioni all'interno di Aries Srl. Il suo scopo è proteggere gli asset informativi dell'organizzazione da tutte le minacce, interne o esterne, intenzionali o accidentali, garantendo la continuità operativa, minimizzando i rischi e massimizzando il ritorno sugli investimenti. Questa politica si applica a tutto il personale, ai processi, ai dati e ai sistemi informativi gestiti da Aries Srl, in conformità con le strategie aziendali,

Riferimenti normativi

- ISO/IEC 27001:2022

Termini e definizioni

- **Riservatezza**: La proprietà che le informazioni non siano rese disponibili o divulgate a individui, entità o processi non autorizzati.
- **Integrità**: La proprietà di salvaguardare l'accuratezza e la completezza degli asset.
- **Disponibilità**: La proprietà di essere accessibile e utilizzabile su richiesta da un'entità autorizzata.

Ruoli e responsabilità

- **Amministratore**: Definisce gli obiettivi strategici per la sicurezza delle informazioni, approva la relativa politica e le sue revisioni, assicura l'assegnazione delle risorse necessarie e promuove una cultura della sicurezza a tutti i livelli aziendali.
- **Responsabile del Sistema di Gestione della Sicurezza delle Informazioni (RSGSI)**: Supervisiona l'implementazione, il mantenimento e il miglioramento continuo del Sistema di Gestione della Sicurezza delle Informazioni, gestisce i rischi, coordina la gestione degli incidenti e assicura la comunicazione delle politiche pertinenti.
- **Personale**: Ha la responsabilità di comprendere e rispettare le politiche di sicurezza aziendali, utilizzare le risorse informative in modo appropriato, proteggere gli asset aziendali e segnalare tempestivamente qualsiasi anomalia o incidente di sicurezza.

Obiettivi di sicurezza delle informazioni

Aries Srl si impegna a proteggere i propri asset informativi per garantire la continuità operativa, la conformità normativa e la tutela della fiducia dei propri clienti e partner. L'Amministratore, in collaborazione con il Responsabile del Sistema di Gestione della Sicurezza delle Informazioni (RSGSI), definisce e riesamina periodicamente gli obiettivi di sicurezza, assicurando che siano allineati con le strategie aziendali e il contesto di riferimento.

Gli obiettivi strategici del Sistema di Gestione della Sicurezza delle Informazioni (SGSI) si fondano sui seguenti pilastri:

- **Riservatezza:** Garantire che le informazioni siano accessibili solo al personale autorizzato. Questo obiettivo è critico per la protezione della proprietà intellettuale delle informazioni commerciali e dei dati del personale.

- **Integrità:** Salvaguardare l'accuratezza, la completezza e la validità delle informazioni e dei metodi di elaborazione. L'integrità è fondamentale per assicurare la qualità e la sicurezza dei prodotti, l'affidabilità dei dati clinici e la correttezza dei processi aziendali.
- **Disponibilità:** Assicurare che il personale autorizzato abbia accesso alle informazioni e alle risorse associate quando necessario. Questo obiettivo supporta la continuità dei processi produttivi, l'erogazione dei servizi di assistenza e le operazioni quotidiane.
- **Conformità:** Garantire il pieno rispetto dei requisiti legali, normativi, statutari e contrattuali applicabili alle attività di Aries Srl.
- **Resilienza:** Migliorare la capacità dell'organizzazione di prevenire, rispondere e ripristinare le operazioni a seguito di incidenti di sicurezza, minimizzando l'impatto sul business.

Questi obiettivi sono misurati e monitorati attraverso indicatori specifici e vengono riesaminati durante il riesame della direzione, come formalizzato nella "PRO Gestione riesame della direzione".

Principi fondamentali di sicurezza delle informazioni

Aries Srl adotta i seguenti principi fondamentali per guidare le decisioni e le attività relative alla sicurezza delle informazioni a tutti i livelli dell'organizzazione.

Impegno della Direzione e Leadership

L'Amministratore dimostra un impegno attivo nel sostenere il SGSI attraverso la definizione della presente politica, l'assegnazione di risorse adeguate e la promozione di una cultura orientata alla sicurezza. L'Amministratore approva formalmente la politica e le sue revisioni.

Approccio basato sul Rischio

Tutte le decisioni e le misure di sicurezza delle informazioni devono essere basate su un processo strutturato di identificazione, valutazione e trattamento dei rischi. L'RSGSI deve supervisionare tale processo in conformità con la "PRO Procedura di gestione dei rischi" per garantire che i controlli siano proporzionati alle minacce identificate.

Responsabilità Condivisa

La sicurezza delle informazioni è una responsabilità condivisa che coinvolge tutto il personale. Ogni dipendente e collaboratore deve comprendere e adempiere ai propri doveri di sicurezza. Le responsabilità specifiche sono formalizzate nella "POL Politica dei ruoli e delle responsabilità in materia di sicurezza delle informazioni" e richiamate nel "Codice di condotta".

Uso Accettabile delle Risorse

Tutto il Personale deve utilizzare le informazioni, i sistemi informativi e gli asset aziendali in modo responsabile, etico e unicamente per gli scopi autorizzati. Le regole per l'uso corretto delle risorse sono dettagliate nella "POL Politica di sicurezza operativa".

Protezione delle Informazioni e degli Asset

Aries Srl adotta i principi di "scrivania pulita e schermo pulito" per ridurre il rischio di accessi non autorizzati, perdita o danneggiamento delle informazioni durante e al di fuori dell'orario di lavoro. Il Personale ha l'obbligo di proteggere adeguatamente gli asset aziendali quando utilizzati fuori sede, in conformità con le direttive specificate nella "POL Politica di sicurezza operativa".

Segnalazione degli Eventi di Sicurezza

Tutto il Personale ha l'obbligo di segnalare tempestivamente qualsiasi evento, anomalia o debolezza di sicurezza osservata o sospetta. L'RSGSI deve garantire che esista un meccanismo di segnalazione chiaro ed efficace, come definito nella "PRO Procedura di gestione degli incidenti di sicurezza delle informazioni".

Miglioramento Continuo

Il SGSI è soggetto a un processo di miglioramento continuo per mantenerne l'adeguatezza, l'idoneità e l'efficacia nel tempo. L'Amministratore, con il supporto dell'RSGSI, guida il riesame periodico delle prestazioni del sistema per identificare opportunità di miglioramento.

Gestione e Comunicazione della Politica

La presente politica e le politiche specifiche per argomento sono approvate dall'Amministratore. L'RSGSI ha la responsabilità di pubblicarle e comunicarle a tutto il Personale e alle parti interessate pertinenti, assicurandone la comprensione e l'accettazione. Le politiche devono essere riesaminate a intervalli pianificati e ogni qualvolta si verifichino cambiamenti significativi, secondo quanto stabilito nella "PRO Gestione riesame della direzione".

Archiviazione e aggiornamenti

Questo documento è archiviato in formato digitale controllato e reso accessibile al personale pertinente. Viene riesaminato con cadenza almeno annuale, o a seguito di cambiamenti significativi nel contesto organizzativo, tecnologico o normativo, per garantirne la continua idoneità, adeguatezza ed efficacia. Le revisioni sono gestite e approvate secondo le procedure aziendali.

Documenti di riferimento

- PRO Gestione riesame della direzione
- PRO Procedura di gestione dei rischi
- POL Politica dei ruoli e delle responsabilità in materia di sicurezza delle informazioni
- Codice di condotta
- POL Politica di sicurezza operativa
- PRO Procedura di gestione degli incidenti di sicurezza delle informazioni