POLITICA
DELLA SICUREZZA DELLE INFORMAZIONI

Rev.	Data	Descrizione	Redazione	Verifica	Approvazione
0	03/07/2023	Prima emissione	RSGSI	RSGSI	AU
1	05/02/2024	Revisione	RSGSI	RSGSI	AU
2	05/11/2024	Revisione	RSGSI	RSGSI	Pres. CDA

1. Obiettivi della politica

Obiettivo del presente documento è quello di delineare i principi generali di sicurezza delle informazioni adottati dalla società Amico Energia S.r.l. al fine di realizzare e mantenere un efficiente e sicuro Sistema di Gestione della Sicurezza delle Informazioni.

Tali principi sono concretizzati nella presente Politica e declinati nel dettaglio nelle politiche e documenti del Sistema di Gestione che descrive le direttive strategiche manageriali volte ad indirizzare la gestione della sicurezza delle informazioni, le cui finalità sono la protezione dei dati e degli elementi del sistema informativo responsabile della loro gestione.

Tali obiettivi fanno riferimento alla necessità di contenere, entro limiti accettabili, il rischio di compromissioni della riservatezza, dell'integrità e della disponibilità delle informazioni aziendali considerate una risorsa di valore strategico per l'organizzazione, la cui tutela rappresenta una precisa responsabilità aziendale sancita anche a livello normativo. In particolare:

- La **tutela della riservatezza** deve attuarsi mediante interventi idonei a contrastare il verificarsi di accessi non autorizzati alle informazioni, o la diffusione non controllata delle stesse;
- La **tutela dell'integrità** deve attuarsi mediante interventi idonei a contrastare il verificarsi di modifiche non autorizzate o il danneggiamento del formato fisico e/o del contenuto semantico delle informazioni;
- La **tutela della disponibilità** deve attuarsi mediante interventi idonei a garantire, ai soggetti autorizzati, l'accesso alle risorse in tempi utili al compimento della propria missione.

Tale tutela va perseguita al fine di mantenere un equilibrio costante nel tempo tra il livello di rischio operativo che l'azienda considera sopportabile e le necessarie misure di protezione, assicurando che la tutela delle informazioni e delle risorse informatiche si traduca anche nella salvaguardia dell'efficienza e dell'efficacia dei processi di erogazione dei servizi di business.

L'impossibilità di garantire alle informazioni aziendali una totale immunità dai rischi intrinseci alle procedure di gestione delle stesse o a quelli derivanti dal tipo di strumento (cartaceo o informatico) utilizzato nell'ambito del trattamento, conduce alla necessità per la Amico Energia di dotarsi di un sistema di contromisure tale da non poter essere eluso se non intenzionalmente, e che consenta di contrastare adeguatamente tali rischi in termini di:

- **Prevenzione** delle minacce e degli attacchi, onde ridurre al minimo la possibilità del verificarsi dei rischi di indisponibilità, accesso non autorizzato e perdita dell'integrità delle informazioni;
- **Reazione** agli attacchi, onde evitarne, contenerne o minimizzarne i danni;
- **Ripristino** della situazione antecedente al verificarsi del danno;

- **Investigazione** per l'analisi e la valutazione dei danni subiti in seguito all'attacco.

La realizzazione e la conseguente gestione di tale sistema, richiede l'indirizzamento di un insieme eterogeneo di interventi, di natura sia tecnologica che organizzativa, atti a garantire il raggiungimento ed il mantenimento nel tempo dei livelli di sicurezza ritenuti adeguati.

L'insieme di tali interventi si configura come un processo continuo di identificazione, analisi e valutazione dei rischi, nonché di selezione delle migliori strategie di prevenzione e gestione degli stessi, volto a consentire il governo della sicurezza del patrimonio informativo aziendale.

La Direzione della Amico Energia si impegna a rendere disponibili le risorse necessarie e funzionali al raggiungimento degli obiettivi di sicurezza delle informazioni prefissati, in termini di:

- Organizzazione;
- Atteggiamento;
- Infrastrutture e know how;
- Sensibilizzazione, consapevolezza e formazione delle persone coinvolte nel Sistema di Gestione per la Sicurezza delle Informazioni.

2. Ambito di applicazione

La Politica Aziendale della Sicurezza delle Informazioni si applica a tutto il personale della Amico energia e a tutti i soggetti che con essa collaborano a vario titolo. Essa si applica, inoltre, a tutti i processi, tra cui l'erogazione dei servizi di teleselling outbound e dei servizi web e voice order, e più in generale a tutte le risorse coinvolte nella gestione delle informazioni trattate dall'Azienda.

La Politica riguarda le modalità di gestione della sicurezza delle informazioni aziendali, nell'accezione più estesa del termine, utilizzate ai fini della loro elaborazione e custodia.

In particolare, le informazioni oggetto di protezione sono relative a:

- Know how tecnico e consulenziale in ambito di teleselling nel settore energia;
- Informazioni di business acquisite direttamente o attraverso il partner primario;
- Informazioni contabili;
- Informazioni sui dipendenti;
- Informazioni su clienti fornitori.

Le risorse cartacee ed informatiche, utilizzate per l'elaborazione e la custodia delle informazioni, cui sono indirizzati gli interventi di tutela, comprendono:

- Documenti contenenti le informazioni aziendali;
- Piattaforme hardware;
- Piattaforme software;
- Infrastrutture di rete e di telecomunicazione;
- Banche dati;
- Documentazione tecnica;
- Applicazioni gestionali e di business;
- Supporti di memorizzazione per la conservazione dei dati.

Informazioni e risorse cartacee ed informatiche utilizzate per l'elaborazione e la custodia delle stesse costituiscono le cosiddette **"Risorse Informative"** aziendali. Le risorse informative devono essere protette dal momento della loro creazione o introduzione in azienda, durante il loro utilizzo, fino al momento della distruzione o dismissione.

La responsabilità di proteggere le risorse informative in rapporto ad eventi, accidentali e/o intenzionali, di distruzione, perdita, divulgazione, alterazione e accesso non autorizzati, spetta all'utilizzatore delle stesse, ovvero al dipendente, nonché ai soggetti terzi (fornitori, consulenti, partner) con cui la Amico Energia intrattiene rapporti professionali.

Tale responsabilità discende dai principi di diligenza e correttezza, che devono indirizzare i comportamenti nell'ambito dello svolgimento delle attività lavorative.

3. Requisiti di conformità

La conformità ai requisiti di sicurezza definiti dalle normative cogenti, dagli standard e dalle best practice applicabili alla Amico Energia risulta imprescindibile nell'ambito del raggiungimento degli obiettivi espressi all'interno della Politica della Sicurezza delle Informazioni.

Tali requisiti sono presi in considerazione nell'ambito della definizione degli obiettivi di sicurezza aziendali e formalizzati all'interno di direttive strategiche che indirizzano la tutela delle risorse informative aziendali.

Tutte le attività dell'Azienda devono essere svolte nell'osservanza della legge, in un quadro di concorrenza leale, per creare valore con integrità per i propri clienti, collaboratori e collettività.

Creare valore con integrità vuol dire agire con onestà, correttezza e buona fede, nel rispetto degli interessi legittimi dei clienti, dei dipendenti, dei partner commerciali e finanziari e delle collettività con cui la Amico Energia si relaziona.

Nell'ambito della definizione delle strategie di gestione della sicurezza delle informazioni, la Amico Energia si pone l'obiettivo di ottemperare ai requisiti derivanti dai principi generali enunciati dall'attuale legislazione italiana nonché a quelli derivanti dalle normative specifiche applicabili ai servizi erogati in materia di:

- Protezione dei dati personali;
- Tutela del software e delle banche dati;
- Criminalità informatica.

La Amico Energia si pone come obiettivo l'adozione di un approccio metodologico alla gestione delle problematiche inerenti alla sicurezza delle informazioni conforme agli standard e alle best practice, nazionali ed internazionali di riferimento per la definizione di ruoli, responsabilità e procedure formali di gestione dei processi sia per l'operatività aziendale che per la trattazione delle emergenze.

4. Direttive strategiche e principali obiettivi

L'instaurazione, l'applicazione, il mantenimento e il miglioramento del Sistema di Gestione della Sicurezza delle Informazioni in accordo alla norma UNI CEI EN ISO/IEC 27001:2022, integrato con l'estensione UNI CEI EN ISO/IEC 270717:2021, si propone attraverso la presente politica i seguenti obiettivi:

- Consolidare ed estendere progressivamente la propria presenza nei mercati di microbusiness, pubbliche amministrazioni e consumer;
- Migliorare continuamente l'efficienza complessiva dell'organizzazione e del Sistema di Gestione della Sicurezza delle Informazioni, assicurando la promozione al proprio interno del rigoroso rispetto di tutte le regole organizzative e procedurali adottate dall'Azienda;
- Assicurare il rispetto delle leggi applicabili, degli impegni contrattuali, degli obblighi di conformità e degli accordi con le parti interessate, nonché dei principi di onestà, trasparenza, lealtà e correttezza;
- Individuare, monitorare e migliorare continuamente le proprie attività per garantire la riservatezza, integrità e disponibilità, e prevenire o ridurre i rischi di natura fisica, logica e organizzativa;

- Incoraggiare e favorire l'attenzione, la consapevolezza e la sensibilizzazione e le competenze in materia di sicurezza delle informazioni;
- Perseguire attraverso le politiche, strumenti e controlli la tutela dei dati personali dei propri dipendenti, dei clienti e delle parti interessate;
- Perseguire attraverso le politiche, strumenti e controlli la tutela dei sistemi informatici, la tutela dell'immagine aziendale e la prevenzione delle frodi;
- Migliorare l'infrastruttura tecnologica e l'organizzazione al fine di incrementare la ridondanza e assicurare la continuità operativa dei servizi e delle informazioni;
- Creare valore aggiunto, attraverso il perseguimento di migliori condizioni economiche, sociali e professionali, nell'ambito della propria specifica attività operativa.

5. Ciclo di vita della politica e responsabilità

La politica viene rivista almeno annualmente in occasione del riesame del Sistema di Gestione della Sicurezza delle Informazioni, definendo obiettivi e traguardi specifici, considerando l'evoluzione del contesto aziendale e l'analisi dei potenziali rischi sulle informazioni, e se del caso, riemessa.

La presente politica viene diffusa attraverso i canali di comunicazione interni alla Amico Energia ed è resa disponibile alle parti interessate tramite il sito internet aziendale: https://www.scegli-tu.com/