	Sistema Gestione Sicurezza dei Dati (SGSD)
arteco	**ALLEGATO 2 - POLITICA AZIENDALE**

La **Politica Aziendale** impone che, in coerenza con la missione aziendale, la gestione di tutti i processi aziendali sia impostata con le regole proprie dell'applicazione del Sistema di gestione secondo la norma **ISO/IEC 27001:2022**.

SCOPO E OBIETTIVI

La direzione di **ARTECO SRL** ha definito, ha divulgato e si impegna a mantenere attiva a tutti i livelli della propria organizzazione la presente politica per la Gestione della Sicurezza delle Informazioni.
Lo scopo della presente policy è di garantire la tutela e la protezione da tutte le minacce, interne o esterne, intenzionali o accidentali, delle informazioni nell'ambito delle proprie attività in accordo con le indicazioni fornite dallo standard ISO/IEC 27001 e dalle linee guida contenute nello standard ISO/IEC 27002 nelle loro ultime versioni.

CAMPO DI APPLICAZIONE

La presente politica si applica indistintamente a tutti gli organi e i livelli dell'Azienda.
L'attuazione della presente politica è obbligatoria per tutto il personale e deve essere inserita nella regolamentazione degli accordi con qualsiasi soggetto esterno che, a qualsiasi titolo, possa essere coinvolto con il trattamento di informazioni che rientrano nel campo di applicazione del Sistema di Gestione (SGSD).
L'azienda consente la comunicazione e la diffusione delle informazioni verso l'esterno solo per il corretto svolgimento delle attività aziendali che devono avvenire nel rispetto delle regole e delle norme cogenti.

POLICY SICUREZZA DELLE INFORMAZIONI

Il patrimonio informativo da tutelare è costituito dall'insieme delle informazioni gestite attraverso i servizi forniti e localizzate in tutte le sedi dell'azienda.
È necessario assicurare:

- la confidenzialità delle informazioni: ovvero le informazioni devono essere accessibili solo da chi è autorizzato.
- l'integrità delle informazioni: ovvero proteggere la precisione e la completezza delle informazioni e dei metodi per la loro elaborazione.
- la disponibilità delle informazioni: ovvero che gli utenti autorizzati possano effettivamente accedere alle informazioni e ai beni collegati nel momento in cui lo richiedono.

La mancanza di adeguati livelli di sicurezza può comportare il danneggiamento dell'immagine aziendale, la mancata soddisfazione del cliente, il rischio di incorrere in sanzioni legate alla violazione delle normative vigenti nonché danni di natura economica e finanziaria.
Un adeguato livello di sicurezza è altresì basilare per la condivisione delle informazioni.
L'azienda identifica tutte le esigenze di sicurezza tramite l'analisi dei rischi che consente di acquisire consapevolezza sul livello di esposizione a minacce del proprio sistema informativo. La valutazione del rischio permette di valutare le potenziali conseguenze e i danni che possono derivare dalla mancata applicazione di misure di sicurezza al sistema informativo e quale sia la realistica probabilità di attuazione delle minacce identificate.

I risultati di questa valutazione determinano le azioni necessarie per gestire i rischi individuati e le misure di sicurezza più idonee.
I principi generali della gestione della sicurezza delle informazioni abbracciano vari aspetti:

- Deve esistere un catalogo costantemente aggiornato degli asset aziendali rilevanti ai fini della gestione delle informazioni e per ciascuno deve essere individuato un responsabile. Le informazioni devono essere classificate in base al loro livello di criticità, in modo da essere gestite con livelli di riservatezza ed integrità coerenti ed appropriati.

- Per garantire la sicurezza delle informazioni, ogni accesso ai sistemi deve essere sottoposto a una procedura d'identificazione e autenticazione. Le autorizzazioni di accesso alle informazioni devono essere differenziate in base al ruolo ed agli incarichi ricoperti dai singoli individui, in modo che ogni utente possa accedere alle sole informazioni di cui necessita, e devono essere periodicamente sottoposte a revisione.
- Devono essere definite delle procedure per l'utilizzo sicuro dei beni aziendali e delle informazioni e dei loro sistemi di gestione.
- Deve essere incoraggiata la piena consapevolezza delle problematiche relative alla sicurezza delle informazioni in tutto il personale (dipendenti e collaboratori) a partire dal momento della selezione e per tutta la durata del rapporto di lavoro.
- Per poter gestire in modo tempestivo gli incidenti, tutti devono notificare qualsiasi problema relativo alla sicurezza. Ogni incidente deve essere gestito come indicato nelle procedure.
- È necessario prevenire l'accesso non autorizzato alle sedi e ai singoli locali aziendali dove sono gestite le informazioni e deve essere garantita la sicurezza delle apparecchiature.
- Deve essere assicurata la conformità con i requisiti legali e con i principi legati alla sicurezza delle informazioni nei contratti con le terze parti.
- Deve essere predisposto un piano di continuità che permetta all'azienda di affrontare efficacemente un evento imprevisto, garantendo il ripristino dei servizi critici in tempi e con modalità che limitino le conseguenze negative sulla missione aziendale.
- Gli aspetti di sicurezza devono essere inclusi in tutte le fasi di progettazione, sviluppo, esercizio, manutenzione, assistenza e dismissione dei sistemi e dei servizi informatici.
- Devono essere garantiti il rispetto delle disposizioni di legge, di statuti, regolamenti o obblighi contrattuali e di ogni requisito inerente la sicurezza delle informazioni, riducendo al minimo il rischio di sanzioni legali o amministrative, di perdite rilevanti o danni alla reputazione.

RESPONSABILITA' DI OSSERVANZA E ATTUAZIONE

L'osservanza e l'attuazione delle policy sono responsabilità di:

1. Tutto il personale che, a qualsiasi titolo, collabora con l'azienda ed è in qualche modo coinvolto con il trattamento di dati ed informazioni che rientrano nel campo di applicazione del Sistema di Gestione. Tutto il personale è altresì responsabile della segnalazione di tutte le anomalie e violazioni di cui dovesse venire a conoscenza.
2. Tutti i soggetti esterni che intrattengono rapporti e collaborano con l'azienda. Devono garantire il rispetto dei requisiti contenuti nella presente policy.

Il Responsabile del Sistema di Gestione che, nell'ambito del Sistema di Gestione e attraverso norme e procedure appropriate, deve:

- condurre l'analisi dei rischi con le opportune metodologie e adottare tutte le misure per la gestione del rischio
- stabilire tutte le norme necessarie alla conduzione sicura di tutte le attività aziendali
- verificare le violazioni alla sicurezza e adottare le contromisure necessarie e controllare l'esposizione dell'azienda alle principali minacce e rischi
- organizzare la formazione e promuovere la consapevolezza del personale per tutto ciò che concerne la sicurezza delle informazioni.
- verificare periodicamente l'efficacia e l'efficienza del Sistema di Gestione.

Chiunque, dipendenti, consulenti e/o collaboratori esterni dell'Azienda, in modo intenzionale o riconducibile a negligenza, disattenda le regole di sicurezza stabilite e in tal modo provochi un danno

all'azienda, potrà essere perseguito nelle opportune sedi e nel pieno rispetto dei vincoli di legge e contrattuali.

RIESAME

La Direzione verificherà periodicamente e regolarmente o in concomitanza di cambiamenti significativi l'efficacia e l'efficienza del Sistema di Gestione, in modo da assicurare un supporto adeguato all'introduzione di tutte le migliorie necessarie e in modo da favorire l'attivazione di un processo continuo, con cui viene mantenuto il controllo e l'adeguamento della policy in risposta ai cambiamenti dell'ambiente aziendale, del business, delle condizioni legali.
Il Responsabile del Sistema di Gestione ha la responsabilità del riesame della politica.
Il riesame dovrà verificare lo stato delle azioni preventive e correttive e l'aderenza alla politica.
Dovrà tenere conto di tutti i cambiamenti che possono influenzare l'approccio della azienda alla gestione della sicurezza delle informazioni, includendo i cambiamenti organizzativi, l'ambiente tecnico, la disponibilità di risorse, le condizioni legali, regolamentari o contrattuali e dei risultati dei precedenti riesami.
Il risultato del riesame dovrà includere tutte le decisioni e le azioni relative al miglioramento dell'approccio aziendale alla gestione della sicurezza delle informazioni.

IMPEGNO DELLA DIREZIONE

La direzione sostiene attivamente la sicurezza delle informazioni in azienda tramite un chiaro indirizzo, un impegno evidente, degli incarichi espliciti e il riconoscimento delle responsabilità relative alla sicurezza delle informazioni.
L'impegno della direzione si attua tramite una struttura i cui compiti sono:

- garantire che siano identificati tutti gli obiettivi relativi alla sicurezza delle informazioni e che questi incontrino i requisiti aziendali;
- stabilire i ruoli aziendali e le responsabilità per lo sviluppo e il mantenimento del SGSD;
- fornire risorse sufficienti alla pianificazione, implementazione, organizzazione, controllo, revisione, gestione e miglioramento continuo del SGSD;
- controllare che il SGSD sia integrato in tutti i processi aziendali e che procedure e controlli siano sviluppati efficacemente;
- approvare e sostenere tutte le iniziative volte al miglioramento della sicurezza delle informazioni;
- attivare programmi per la diffusione della consapevolezza e della cultura della sicurezza delle informazioni.

Faenza (RA), lì **09.12.2025**

DGE GIAMPAOLO SABBATANI 27/04/2026 15:39:25 UTC+0200

The **Corporate Policy** requires that, in alignment with the Company's mission, all business processes are managed in accordance with the rules and principles of a Management System compliant with **the ISO/IEC 27001:2022 standard.**

PURPOSE AND OBJECTIVES

The Management of **ARTECO SRL** has defined, communicated, and is committed to maintaining this Information Security Policy active at all levels of the organization.

The purpose of this Policy is to ensure the protection of information against all threats, whether internal or external, intentional or accidental, within the scope of company activities, in accordance with the requirements of the ISO/IEC 27001 standard and the guidelines set out in ISO/IEC 27002, in their latest versions.

SCOPE

This Policy applies to all organizational units and levels of the Company without exception.

Compliance with this Policy is mandatory for all personnel and must be incorporated into contractual arrangements with any external party that, in any capacity, may be involved in the processing of information falling within the scope of the Information Security Management System (ISMS).

The Company permits the communication and dissemination of information to external parties solely for the proper execution of business activities and in compliance with applicable laws, regulations, and binding requirements.

INFORMATION SECURITY POLICY

The information assets to be protected consist of all information managed through the services provided and located across all Company sites.

The following principles must be ensured:

- Confidentiality of information: information must be accessible only to authorized individuals.
- Integrity of information: the accuracy and completeness of information and processing methods must be safeguarded.
- Availability of information: authorized users must have access to information and associated assets when required.

Failure to ensure adequate levels of security may result in damage to the Company's reputation, customer dissatisfaction, exposure to legal sanctions due to non-compliance with applicable regulations, as well as economic and financial losses.

An adequate level of security is also essential for the proper sharing of information.

The Company identifies all security requirements through risk analysis, which enables awareness of the exposure level of its information system to threats. Risk assessment allows the evaluation of potential consequences and damages arising from the failure to implement security measures, as well as the likelihood of occurrence of identified threats.

The results of this assessment determine the actions required to manage identified risks and the most appropriate security measures to be adopted.

General principles of information security management include:

- A continuously updated inventory of information assets shall be maintained, with a designated owner for each asset. Information shall be classified according to its level of criticality to ensure appropriate confidentiality and integrity controls.
- Access to systems shall be subject to identification and authentication procedures. Access rights shall be assigned based on roles and responsibilities and periodically reviewed to ensure that users access only the information necessary for their duties.

- Procedures for the secure use of company assets, information, and information systems shall be defined.
- Awareness of information security issues shall be promoted among all personnel (employees and collaborators), starting from recruitment and throughout the employment relationship.
- All personnel shall promptly report any information security incidents or weaknesses. Incidents shall be managed in accordance with established procedures.
- Unauthorized physical access to Company premises and areas where information is processed shall be prevented, and equipment security shall be ensured.
- Compliance with legal requirements and information security principles shall be ensured in agreements with third parties.
- A business continuity plan shall be established to enable the Company to effectively respond to unforeseen events and ensure the timely restoration of critical services, minimizing impacts on business operations.
- Security requirements shall be integrated into all phases of the lifecycle of information systems and services, including design, development, operation, maintenance, support, and decommissioning.
- Compliance with applicable laws, regulations, contractual obligations, and all information security requirements shall be ensured, minimizing the risk of legal or administrative sanctions, significant losses, or reputational damage.

RESPONSIBILITIES FOR COMPLIANCE AND IMPLEMENTATION

Compliance with and implementation of this Policy are the responsibility of:

1. All personnel who, in any capacity, collaborate with the Company and are involved in processing information within the scope of the ISMS. All personnel are also responsible for reporting any anomalies or violations.
2. All external parties who have relationships or collaborations with the Company and must ensure compliance with the requirements set out in this Policy.

The Information Security Management System Manager, within the scope of the ISMS and through appropriate rules and procedures, shall:

- Conduct risk analysis using appropriate methodologies and implement risk treatment measures;
- Establish all necessary rules for the secure execution of business activities;
- Monitor security breaches, implement corrective actions, and oversee the Company's exposure to threats and risks;
- Organize training and promote awareness regarding information security;
- Periodically verify the effectiveness and efficiency of the ISMS.

Any employee, consultant, or external collaborator who intentionally or negligently violates the established security rules and causes damage to the Company may be subject to disciplinary and/or legal action, in accordance with applicable laws and contractual provisions.

MANAGEMENT REVIEW

Top Management shall periodically review, or review upon significant changes, the effectiveness and efficiency of the ISMS to ensure adequate support for continuous improvement and adaptation to changes in the business environment, operations, and legal conditions.

The ISMS Manager is responsible for reviewing this Policy.

The review shall assess the status of preventive and corrective actions and compliance with the Policy. It shall consider all changes that may affect the Company's approach to information security management, including organizational changes, technological environment, resource availability, legal, regulatory, or contractual requirements, as well as the results of previous reviews.

The outcome of the review shall include decisions and actions related to the continual improvement of the Company's information security management approach.

MANAGEMENT COMMITMENT

Top Management actively supports information security through clear direction, demonstrated commitment, defined roles, and assigned responsibilities.

Management commitment is implemented through a structure responsible for:

- Ensuring that information security objectives are defined and aligned with business requirements;
- Establishing roles and responsibilities for the development and maintenance of the ISMS;
- Providing adequate resources for planning, implementation, operation, monitoring, review, management, and continual improvement of the ISMS;
- Ensuring that the ISMS is integrated into all business processes and that procedures and controls are effectively developed;
- Approving and supporting initiatives aimed at improving information security;
- Promoting awareness and a culture of information security throughout the organization.

Faenza (RA), **09 December 2025**

DGE _____

GIAMPAOLO
SABBATANI
27/04/2026 15:39:27 UTC+0200