POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

- Information Security Policy -

ATTENZIONE !!

a) Distribuzione in formato Elettronico su rete LAN aziendale,
b) Versione non controllata se stampata su supporto cartaceo o su copia di file salvato in locale.

4 settembre 2023	Rev. 2	Adeguamento Riferimenti Normativi	S. Cirimelli	F. Scalesse
1° agosto 2023	Rev. 1	Integrazione Obiettivi	S. Cirimelli	F. Scalesse
15 gennaio 2022	Rev. 0	Prima Emissione	S. Cirimelli	F. Scalesse
Data	**Revisione**	**Motivo**	**Emissione**	**Approvazione**

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

La politica per la sicurezza delle informazioni gestite da *ESINWARE S.r.l*. ha l'obiettivo di fornire la linea guida a tutta l'organizzazione aziendale allo scopo di proteggere il patrimonio informativo da tutte le minacce prevedibili: organizzative, tecnologiche e sociali - siano esse (Interne / Esterne), (Nazionali / Internazionali), (Deliberate / Accidentali).

Il vertice della direzione di *ESINWARE* intende:

- garantire la riservatezza delle informazioni,
- mantenere l'integrità delle informazioni,
- assicurare la disponibilità delle informazioni,
- garantire l'Autenticità delle informazioni,
- rispettare i requisiti legislativi / normativi e contrattuali,
- Conservare fino a restituzione le informazioni / i documenti affidategli da terzi.

Gli obiettivi di sicurezza vengono perseguiti attraverso un adeguato piano di investimenti per la prevenzione di eventi avversi malevoli e/o accidentali.

Il coinvolgimento dei collaboratori di *ESINWARE*, ritenuto fondamentale per il rispetto della stessa policy, passa attraverso un piano di formazione di tutto il proprio personale per renderlo edotto e consapevole della criticità insita nella custodia e nella manipolazione dei dati di terzi.

L'efficacia delle attività di monitoraggio delle tentate violazioni, Fisiche e Logiche e di tutti gli eventi avversi di cui si individua una traccia, passa attraverso l'applicazione sistematica delle procedure del sistema di gestione per la sicurezza dei dati: SgSI implementato dall'organizzazione di *ESINWARE*.

L'assunzione di responsabilità da parte di tutto il management e l'impegno al controllo sistematico della corretta applicazione delle procedure stabilite è la sola via che può assicurare ai clienti il livello di garanzia che si attendono e che *ESINWARE* hanno consapevolmente accettato di garantire.

Uso Confidenziale - Vietato Ogni Utilizzo non Formalmente Autorizzato
Proprietà ESINWARE S.r.l.

Il management e l'intera organizzazione di *ESINWARE* strutturano l'intero sistema di Prevenzione e Protezione dei rischi da minacce interne ed esterne in base alla tipologia e criticità del set di dati trattati e conservati. Pur avendo l'obiettivo di trattare e conservare tutti i dati nel pieno rispetto dei diritti degli interessati e nel rispetto della legislazione vigente, il management di *ESINWARE* porrà particolare attenzione alle precauzioni da adottare al fine di garantire la (Disponibilità, Integrità e Riservatezza) di talune informazioni industriali e personali (anche sensibili quali ad esempio quelli Giudiziari e Sanitari o relative a minori) e quelle "Particolari" (Sindacali / Politiche, Religiose), in tutte le fasi coinvolte dal trattamento per la conduzione di una commessa.

La figura di Rappresentante della direzione di *ESINWARE* per la Gestione della sicurezza delle Informazioni è mantenuta dall'Amministratore Unico di *ESINWARE* (Dr. Francesco Scalesse) con l'incarico di stimolare la corretta applicazione della politica di data security a cui l'organizzazione deve fare riferimento.

Responsabile del Sistema di Gestione per la Sicurezza delle informazioni di *ESINWARE* è stato nominato *l'Ing. Severino Cirimelli* che all'interno dell'organizzazione aziendale ha il compito di implementare il sistema di gestione, di renderlo e mantenerlo conforme alla normativa di riferimento UNI EN ISO /CEI 27001: 2022. Egli deve monitorare la sua corretta applicazione in tutti i processi aziendali che hanno impatto sulla sicurezza delle informazioni trattate.

MODALITÀ OPERATIVE PER L'ATTUAZIONE DELLA POLICY AZIENDALE PER LA SICUREZZA DELLE INFORMAZIONI CONFERITE DAI CLIENTI

La policy per la sicurezza dei dati dei clienti ed egli altri soggetti interessati che *ESINWARE* trattano nei loro sistemi informativi è mantenuta attiva, verificata e revisionata nel tempo. La policy aziendale di *ESINWARE* è ispirata ai principi della norma internazionale ISO 27001 per la sicurezza delle informazioni.

La policy di sicurezza viene assicurata attraverso il mantenimento in buono stato di manutenzione dei Sistemi di protezione fisica, attivi e passivi degli immobili che ospitano gli asset con cui vengono trattati dati personali ed industriali propri e di terzi.

La regolamentazione degli accessi sia del personale interno che dei soggetti terzi a tali sedi è uno dei pilastri del livello di sicurezza che *ESINWARE* intende mantenere.

la sicurezza logica viene mantenuta attiva grazie ai sistemi di protezione contro malware e virus nonché da tentativi di intrusione fraudolenta.

SISTEMI DI PROTEZIONE PASSIVA:

Il sistema di protezione passiva è garantito con:

- la Recinzione dell'intera area su cui sorge la sede e le infrastrutture.
- la presenza delle Grate metalliche e/o serrature blindate sulle porte facilmente accessibili.

Gli stessi elementi protettivi sono verificati giornalmente dal controllo del personale responsabile della sede finalizzato ad assicurarsi della loro integrità. In caso venissero riscontrate anomalie durante il controllo, verrebbero coinvolti i fornitori convenzionati che sono in grado di intervenire in tempi rapidi, in primis l'istituto di vigilanza convenzionato localmente ed il servizio di portierato dove presente.

SISTEMI DI PROTEZIONE ATTIVA:

la protezione attiva è invece assicurata dalla presenza di:

- un sistema di allarme antintrusione perimetrale interno,
- un sistema di videosorveglianza con registrazione continua H24,

- un servizio di portierato.

Gli stessi sistemi protettivi sono verificati giornalmente dal personale responsabile di sistema di *ESINWARE* che registra ogni anomalia riscontrata in fase di apertura e di chiusura. In fase di chiusura si allontana soltanto dopo essersi assicurato della piena funzionalità dei presidi di sicurezza. In caso venissero riscontrate anomalie durante la giornata o in fase di apertura e chiusura, verrebbero coinvolti i fornitori convenzionati che sono in grado di intervenire in tempi rapidi anche con assistenza in remoto sui sistemi tecnologici di protezione.

GESTIONE DEGLI ACCESSI:

Le policies aziendali mantenute attive nell'organizzazione di *ESINWARE* prevedono un ferreo controllo sul flusso di accesso in ogni sede e ciò vale sia per il personale interno che per i soggetti esterni che a vario titolo potrebbero avere necessità di accedere ai locali della sede locale.

Controllo del Personale Interno:

Per regolamentare l'accesso del personale interno di *ESINWARE* è stato rilasciato un formale incarico per autorizzare ogni risorsa al trattamento dei dati, limitatamente a quanto previsto dalla mansione e/o dal progetto ad essa assegnato. L'incarico è accompagnato da una adeguata attività formativa e di sensibilizzazione sulle criticità legate al ruolo che esse ricoprono all'interno della sede e durante lo svolgimento delle attività ad essa connesse, come progettazione segregazioni di rete, programmazione software, assistenza clienti, e servizi svolti direttamente presso i clienti.

Per ogni dipendente / collaboratore autorizzato ad accedere alle sedi di *ESINWARE o alle sedi di terzi per suo conto*, viene conservata la registrazione cartacea / informatica degli accessi eseguiti per ogni singola giornata di presenza in sede e/o di attività svolta in esterno.

Controllo dei soggetti Esterni:

Per il controllo degli accessi dei soggetti esterni viene invece seguito con una specifica procedura applicata a tutti i soggetti terzi coinvolti da *ESINWARE* quali: Clienti, Fornitori, Enti di controllo, Autorità, etc. per i quali è giustificata la necessità di accesso alla singola sede. La procedura operativa per il controllo accessi prevede:

- Autorizzazione all'accesso a cura del responsabile del trattamento dei dati e/o del referente a seguito dell'analisi della motivazione che accompagna la richiesta di accesso,
- sottoscrizione preventiva del vincolo di riservatezza sottoscritto dal soggetto che è stato autorizzato all'accesso in azienda,
- Accettazione del divieto di effettuare Riprese video e fotografiche con preventivo spegnimento dei dispositivi personali e/o loro consegna all'ingresso prima dell'accesso,
- Accettazione del divieto di raccogliere informazioni scritte o verbali sulla natura dei dati custoditi / trattati ad eccezione eventualmente di quelli di proprietà *(vale soltanto per le visite di personale dei clienti*),
- Registrazione del singolo accesso in sede con la dettagliata raccolta degli estremi dell'identificazione avvenuta a carico del responsabile di sede,
- Accompagnamento pedissequo dell'ospite durante la sua permanenza nella sede aziendale di *ESINWARE* a cura del responsabile o di un altro operatore da esso incaricato.

IDENTIFICAZIONE DEI DATI PRESENTI NELLE SEDI:

In fase di progettazione del singolo servizio offerto ai clienti da parte di *ESINWARE* sono previste alcune precauzioni finalizzate a rendere impossibile o comunque non immediata l'identificazione delle informazioni trattate e dove concordato con i clienti stessi, anche l'anonimato dei clienti proprietari dei dati stessi. Nelle singole aree i dati potrebbero essere identificabili esclusivamente con un codice alfanumerico univoco associato al singolo asset che ne permette la rintracciabilità ma non la diretta identificazione del loro contenuto su indicazione dello stesso cliente titolare del trattamento.

Del singolo accesso ai DB di *ESINWARE*, inoltre viene tenuta traccia dal server che governa la rete LAN ed il DB e che consente al singolo operatore soltanto il permesso di accedere ai dati per cui risulta profilato secondo le indicazioni del responsabile del progetto del cliente.

Il personale di *ESINWARE* è inoltre tenuto ad osservare dettagliate procedure di controllo sia in apertura che in chiusura della sede a cui accede per primo al fine di prevenire situazioni di deficit protettivo che potrebbero permettere facili violazioni durante gli orari non lavorativi. In tali orari notturni e festivi, comunque, la sicurezza potrebbe essere assicurata dal servizio di vigilanza affidato al servizio di metronotte.

Il Responsabile della Protezione dei dati (DPO) si assicura del rispetto di tali procedure sia attraverso pianificate visite Ispettive Interne e sia attraverso l'analisi degli eventi avversi registrati e segnalati.

GESTIONE DELLA CRITICITÀ DELLE INFORMAZIONI

La protezione dei dati viene attuata sulla base della loro criticità, valore e sensibilità. Le specifiche procedure operative riportano i dettagli per l'attuazione delle misure fisiche e logiche della protezione tenendo conto dell'impatto che ogni vulnerabilità può avere sugli interessati:

- Valore Economico aziendale per il cliente;
- Vantaggio Competitivo per segreto aziendale e know-how;
- Discriminazione Raziale / Sociale per le persone fisiche interessate;
- Penalizzazione personale per divulgazione indebita di notizie sullo stato di salute, Preferenze Sessuali, credenza religiosa, pensiero politico etc.

SERVIZI IN CLOUD (SaaS):

L'intera organizzazione di *ESINWARE* è impegnata nella creazione di nuovi servizi da erogare in modalità SaaS via web poggiati sulle infrastrutture IT esterne di service provider terzi convenzionati, selezionati in base a specifiche necessità operative e/o strategiche. I responsabili di *ESINWARE* coinvolti nella progettazione / Sviluppo / Erogazione dei servizi in cloud (SaaS), garantiscono la sicurezza delle informazioni coinvolte (sia Industriali che Personali – PII) tenendo conto dei singoli aspetti di sicurezza che caratterizzano ogni servizio SaaS erogato alla clientela:

- Impatto dei requisiti di sicurezza delle informazioni di base, da prendere in considerazione già in fase di progettazione e implementazione del singolo servizio cloud come:

- Gestione dei rischi legati ai componenti dell'organizzazione;

- Gestione dell'isolamento dei dati multi-tenancy del servizio cloud erogato ai clienti (compresa la virtualizzazione);

- Gestione dell'accesso alle informazioni dei clienti del servizio cloud da parte di fornitori coinvolti da *ESINWARE* nell'erogazione di servizi cloud;

- Gestione della necessità di autenticazione forte per l'accesso con profili di amministratore dei servizi cloud;

- Gestione della necessità di comunicazione ai clienti del servizio cloud durante il rilascio di modifiche con impatto funzionale;

- Gestione della sicurezza legata alla virtualizzazione dei server;

- Gestione dell'accesso e della protezione dei dati dei clienti del servizio cloud;

- Gestione della gestione del ciclo di vita degli account dei clienti del servizio cloud;

- Gestione della comunicazione di avvenute violazioni delle informazioni trattate.

OPERATIVITÀ IN REMOTO DEL PERSONALE (Smart Working):

L'intera organizzazione di *ESINWARE* è impegnata nel garantire la continuità del servizio anche nel nuovo paradigma conseguente al periodo pandemico che ha portato alla formulazione della modalità di lavoro da remoto. Il personale è formato e sensibilizzato sui corretti comportamenti da tenere al fine di rispettare i livelli di sicurezza delle informazioni trattate in fase di erogazione dei servizi interni o a terzi. Le condizioni comportamentali e gli impegni di riservatezza relativi alle attività da remoto sono contenute in specifiche policies sottoscritte da ogni dipendente.

La direzione di *ESINWARE* Rinnova la propria fiducia per il prossimo esercizio all'incaricato *Severino Cirimelli* quale Responsabile del SgSI di *ESINWARE* ed incaricato dell'implementazione e del mantenimento del sistema stesso, compresa la verifica della conformità verso l'evoluzione degli standard di riferimento e della legislazione applicabile.

Roma4 settembre 2023

Francesco Scalesse
Amministratore Esinware S.r.l.