Sistema di Gestione per la Sicurezza delle Informazioni, conforme alla norma ISO IEC 27001:2022 e ISO IEC 9001:2015

Politica aziendale della Sicurezza delle Informazioni e sulla Qualità

Redatto da:	ISMS Manager Quality Manager	Marco Saccani Odelia Barbieri	18/09/2024 Data
Approvato da:	CEO	Federico Germi	18/09/2024 Data

Codice documento:	SGSI_Politica aziendale della Sicurezza delle Informazioni e della Qualità
Revisione	Rev.3 del 18/09/2024
Distribuzione:	CONTROLLATA

STORIA DELLE MODIFICHE APPORTATE

Revisione	Data	Modifica
Rev.1	24/11/2023	Prima emissione
Rev.2	23/01/2024	Aggiunta obiettivo certificazione ACN
Rev.3	18/09/2024	Aggiunta di nuovi obiettivi dell'azienda in merito alla sicurezza e alla salvaguardia dell'ambiente

Tutti i diritti riservati.

SOMMARIO

SOMMARIO *3*
INDICE DELLE FIGURE *3*
1. GENERALITA' *4*
2. TERMINI E DEFINIZIONI *4*
3. PARTE PRINCIPALE *5*

INDICE DELLE FIGURE

Non è stata trovata alcuna voce dell'indice delle figure.

Tutti i diritti riservati.

1. GENERALITA'

1.1 Scopo

Scopo della presente politica è quello di descrivere gli obiettivi di alto livello emanati dalla Direzione in merito all'impegno nei confronti della gestione del sistema per la Sicurezza delle Informazioni e della Qualità.

1.2 Applicazione

Questo documento è applicabile a tutti i processi aziendali.

1.3 Validità e decorrenza

Il presente documento è valido dalla data di approvazione.

1.4 Allegati

Nessuno.

1.5 Riferimenti

Nessuno.

2. TERMINI E DEFINIZIONI

Acronimo/ Termine	Testo esplicativo della definizione
ISMS	**Information Security Management System** E' il Sistema di Gestione per la Sicurezza delle Informazioni (SGSI), di cui tale politica è parte, e la cui redazione è stata pianificata sulla base dei requisiti della normativa ISO/IEC 27001:2022

Tutti i diritti riservati.

3. PARTE PRINCIPALE

Ilger.com S.r.l. (di seguito Ilger) ritiene che la qualità dei processi e la sicurezza delle informazioni debbano concorrere se si vuole erogare un servizio di eccellenza verso il Cliente, la cui soddisfazione è, da sempre, il driver principale di ogni scelta aziendale.

Ilger **dichiara** quindi il proprio impegno a realizzare e mantenere un Sistema Integrato per la Sicurezza delle Informazioni, dei dati personali e della Qualità, perseguendo un continuo miglioramento dei processi posti in essere per l'erogazione dei servizi ai propri clienti, con l'obiettivo tra l'altro di:

- Garantire la massima sicurezza delle informazioni dei clienti, in termini di riservatezza, disponibilità e integrità delle informazioni e dei dati personali (con particolare attenzione alla conformità rispetto al Regolamento UE 2016/679 sulla Protezione dei Dati Personali) stessi fornendo così un servizio ad alto valore aggiunto.
- Garantire requisiti di qualità, di sicurezza, di performance e scalabilità, di interoperabilità e portabilità dei servizi cloud per la PA (QC1) secondo i parametri definiti da ACN (Agenzia per la Cybersicurezza Nazionale);
- Erogare servizi in linea con le aspettative dei Clienti, in termini di rispetto delle tempistiche e livelli di servizio concordati.
- Erogare servizi innovativi in linea con gli sviluppi tecnologici, anticipando le necessità e le aspettative dei clienti.
- Dare continuità operativa ai servizi critici anche a seguito di gravi incidenti potenzialmente capaci di compromettere la sopravvivenza dell'azienda stessa.
- Assumere come priorità la qualità della relazione con il cliente riconoscendo inoltre l'importanza dei rapporti coi fornitori e della loro valorizzazione, nell'ottica di una crescita comune.

Ilger **si impegna**, anche attraverso la partecipazione dei propri dipendenti ad assicurare la qualità ed il miglioramento continuo del servizio, la tutela dei dati, anche in funzione di disposizioni legislative, il rispetto delle Procedure Aziendali e di ogni altro accordo sottoscritto con le parti interessate.

Ilger **persegue** il miglioramento continuo del suo Sistema di Gestione Integrato, individuando i seguenti principi:

Tutti i diritti riservati.

- Fornire un servizio di supporto fondamentale al Core Business dell'impresa attraverso strumenti e mezzi tecnologicamente in linea con il progresso e mantenendoli in perfetto stato di efficienza;
- Definire ruoli e responsabilità del personale coinvolto nella gestione della Data Protection, della Sicurezza delle Informazioni e della Qualità;
- Definire ruoli e responsabilità dell'organizzazione in merito ai trattamenti di dati personali effettuati, anche stipulando gli opportuni accordi in tema di protezione dei dati personali.
- Identificare in modo periodico i potenziali rischi e opportunità che potrebbero presentarsi, provvedendo a pianificare ed attuare idonee azioni volte ad affrontarli e a garantire il normale proseguimento delle attività dell'impresa e a migliorare l'efficacia del Sistema di Gestione;
- Identificare in modo periodico e sistematico le minacce incombenti sui dati, valutandone le esposizioni ai rischi specifici di perdita di riservatezza, integrità e di disponibilità dei dati e provvedendo ad attuare idonee azioni preventive;
- Garantire, anche con l'ausilio del DPO (Data Protection Officer), la conformità delle operazioni di trattamento di dati personali alle norme applicabili in materia, nonché al Regolamento UE 2016/679, anche attraverso l'effettuazione di audit privacy periodici;
- Formare il personale nello svolgimento delle attività in modo da proteggere gli asset aziendali e valutare e riconoscere il valore professionale ed umano dei propri dipendenti come patrimonio aziendale impegnandosi in un costante accrescimento dello stesso;
- Incoraggiare la diffusione della cultura e sensibilizzazione alla sicurezza e protezione dei dati e delle informazioni ed al rispetto delle Procedure volte al perseguimento della Qualità dei servizi resi dall' Azienda ed al loro continuo miglioramento;
- Far fronte con rapidità, efficacia e scrupolo a emergenze o incidenti che possano verificarsi nello svolgimento delle attività, collaborando anche con terze parti o Enti preposti;
- Garantire la definizione e il pieno rispetto delle procedure previste dal Regolamento UE 2016/679 in materia di gestione di violazioni di dati personali (Data Breach);

Tutti i diritti riservati.

- Rispettare le leggi e i regolamenti in vigore nel mercato di riferimento, e comunque attenersi a standard individuati con senso di responsabilità e consapevolezza, basati su principi scientifici e di valutazione dei rischi, assicurando così la conformità dei propri servizi sia ai requisiti di legge sia a ulteriori requisiti necessari per garantire piena soddisfazione del cliente.
- Effettuare attività di controllo e riesame sulle attività svolte e sui trattamenti dei dati personali effettuati, a partire da quelli più critici al fine di mantenere una costante efficienza dei sistemi coinvolti nell' erogazione dei servizi
- Considerare l'importanza di mantenere una pronta risposta all'evolversi del mercato mediante un'organizzazione flessibile e competitiva, sempre attenta alle novità ed al miglioramento della propria offerta.
- Adottare un approccio per processi nella strutturazione delle attività, in quanto identificato dagli standard internazionali quale approccio efficace per garantire qualità ed efficienza dei servizi.
- Riconoscere il valore professionale ed umano dei propri dipendenti come patrimonio aziendale ed impegnarsi ad un costante accrescimento, impegnandosi in una costante azione di motivazione e formazione delle risorse umane.
- Assicurare a clienti e altri stakeholder massima qualità dei servizi offerti, anche grazie all'adozione di un sistema di controllo degli approvvigionamenti esterni, documentato con la compilazione di schede di valutazione dei fornitori.
- Minimizzare i rischi riguardo alla qualità di servizi, erogati attraverso eventuali terze parti coinvolte attraverso la regolamentazione dei rapporti con i fornitori utilizzati; qualora le terze parti trattino dati personali si procederà alla sottoscrizione di Accordi contrattuali relativi al trattamento dei dati, definendo le opportune misure di sicurezza che il fornitore dovrà garantire.
- Riconoscere che la qualità della propria gestione è determinante per la realizzazione del Business aziendale, e per la creazione di valore per i propri Clienti. Impegnarsi a pianificare, sviluppare, aggiornare e comunicare gli obiettivi del Sistema di Gestione al fine di migliorarne l'attuazione.
- Assicurarsi che tutto il personale di qualunque livello ne comprenda e rispetti gli obiettivi posti dal Sistema di Gestione.
- Impegnarsi a fornire servizi nel rispetto dell'ambiente e del climate change.

In particolare, con riferimento ai servizi Zimbra in cloud, ILGER **si impegna** a mantenere un livello elevato di sicurezza, curando in particolare aspetti quali:

Tutti i diritti riservati.

- accessi logici agli applicativi e alle infrastrutture;
- gestione degli asset adeguata e aggiornata;
- mantenere una infrastruttura di rete protetta e sicura, in linea con gli standard del tempo;
- gestione delle richieste e degli incidenti in modo coerente ed efficace;
- gestione strutturata dei log, conservazione in maniera protetta e loro monitoraggio regolare;
- gestione controllata delle attività atte a garantire la riservatezza, l'integrità e la disponibilità delle informazioni come backup, controllo crittografici su informazioni critiche, effettuazione di test prima di procedere con cambiamenti degli ambienti di produzione, ecc.;
- adozione di un piano di business continuity per garantire la continuità operativa;
- verifica periodica della sicurezza degli ambienti utilizzati con attività di vulnerability assessment e/o penetration test.

La Direzione ha identificato il proprio Rappresentante incaricato di gestire il Sistema di Gestione della Sicurezza delle Informazioni (Responsabile della Sicurezza delle Informazioni o ISMS Manager) e un *Quality Manager* incaricato di gestire il Sistema di Gestione della Qualità dei processi aziendali.
L'organizzazione ha nominato un DPO (Data Protection Officer), in modo da supportare Ilger nell'adeguamento agli obblighi previsti dalla normativa in materia di protezione dei dati personali introdotti dal Regolamento UE 2016/679

La Direzione si impegna a revisionare periodicamente la presente Politica con lo scopo di mantenerla in linea con il contesto in cui Ilger opera.

"Il raggiungimento dei suddetti obiettivi è possibile con il coinvolgimento e la collaborazione di ognuno di noi."

La Direzione di
Ilger.com S.r.l.

Tutti i diritti riservati.