E-Time s.r.l.
Viale del Lavoro, 45
37036 - San Martino Buon Albergo (VR)
Italy

P.IVA: 03256040233
Tel. +39 045 8780289
e-mail: info@e-time.it
Web: www.e-time.it

Politica per la Sicurezza delle Informazioni

Storico del documento

Rev.	Data	Autore	Motivo della revisione	Approvato da:
0	17/03/2023	Raffaele	Bozza	Direzione
1	25/05/2023	Gruppo SGSI	Approvazione	Direzione
2	15/05/2024	Gruppo SGSI	Riesame completo del documento e sezione 8 obiettivo su aspetti del cambiamento climatico	Direzione

SOMMARIO

1 Premessa

La presente Politica ha lo scopo di fornire un orientamento gestionale ed un supporto per la corretta gestione della sicurezza delle informazioni.

La sicurezza del patrimonio informativo costituisce la condizione determinante per il raggiungimento degli obiettivi della Direzione della Società E-time.

I requisiti per la sicurezza delle informazioni sono coerenti con gli obiettivi dell'organizzazione e il Sistema di Gestione della Sicurezza delle Informazioni (di seguito anche definito SGSI), di cui questa Politica è parte integrante. Tale Sistema rappresenta lo strumento che consente la condivisione delle informazioni, lo svolgimento di operazioni appropriate e la riduzione dei rischi connessi alle informazioni trattate nell'ambito di riferimento a livelli accettabili.

Pertanto, lo svolgimento delle attività dell'organizzazione E-time deve sempre avvenire garantendo adeguati livelli di riservatezza, integrità e disponibilità delle informazioni, attraverso l'adozione di un formale "Sistema di Gestione della Sicurezza delle Informazioni" in linea con i requisiti attesi dalle parti interessate (anche definiti stakeholder) di E-time ed in conformità alle normative vigenti applicabili.

2 Diffusione e riservatezza del documento

Il presente documento è considerato "Pubblico" in quanto contiene informazioni e riferimenti di governo delle questioni relative alla sicurezza delle informazioni che possono essere comunicate liberamente, senza che vi possano essere conseguenze pregiudizievoli per E-time o che proprio per le loro caratteristiche di promozione e conoscenza devono essere comprese e diffuse senza limitazioni o esclusioni.

3 Riferimenti normativi, standard e modelli

Molti aspetti della sicurezza delle informazioni sono normati dalla legislazione italiana ed europea; alla data della presente revisione, di seguito sono riportate le fonti principali di riferimento normativo, regolamenti, standard e linee guida che si ritengono più rilevanti per

mantenere e migliorare la gestione degli aspetti di sicurezza delle informazioni.

- ISO/IEC 27001: 2022 – Information security management systems – Requirements;
- UNI CEI EN ISO/IEC 27001:2024 - Sicurezza delle informazioni, cybersecurity e protezione della privacy - Sistemi di gestione per la sicurezza delle informazioni - Requisiti
- ISO/IEC 27002: 2022 - Information security, cybersecurity and privacy protection — Information security controls;
- ISO/IEC 27017:2015 - Code of practice for information security controls based on ISO/IEC 27002 for cloud services;
- ISO/IEC 27018:2019 - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors;
- ISO/IEC 27005:2022 - Guidance on managing information security risks;
- Regolamento UE 2016/679 – Regolamento Generale sulla Protezione dei Dati (GDPR);
- Decreto Legislativo del 30 giugno 2003, n.196 e s.m.i. (Codice Privacy);
- Legge 4 agosto 2021, n. 109 - Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale;
- Regolamento (UE) 2019/881 (Cybersecurity Act);
- LEGGE 28 giugno 2024, n. 90 - Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici;
- Cloud Security Alliance (CSA);
- Direttiva (UE) 2022/2555 del 14 dicembre 2022 (Direttiva NIS2);
- Indicazioni dell' European Union Agency for Cybersecurity (ENISA);
- Provvedimenti dell'Agenzia di Cybersecurity Nazionale (ACN);
- Provvedimenti dell'Agenzia per l'Italia Digitale (AgID);
- Framework di Cybersecurity Nazionale (FNCS), ispirato al Cybersecurity Framework ideato dal NIST (National Institute of Standards and Technology).

4 PROFILO DELLA SOCIETÀ

E-time srl è una societa informatica fondata del 2002 con sede principale a San Martino Buon Albergo (VR).

L'azienda è diventata negli anni una realtà consolidata nello sviluppo di soluzioni software per il mondo bancario e assicurativo, oltre ad offrire servizi di consulenza, formazione e assistenza.

E-Time è in particolare specializzata nello studio e nella realizzazione di progetti di integrazione tra sistemi software (System Integration).

L'azienda è costituita da una trentina di specialisti nel settore ICT suddivisi tra la sede principale di San Martino Buon Albergo (VR) e la sede operativa di Capurso (BA).

La mission della società è quella di affiancare i propri Clienti, in modo onesto e trasparente, nel percorso tecnologico per portare innovazione, evoluzione e semplificazione, affinché i loro bisogni trovino una risposta efficace e di valore.

I Clienti di E-time operano principalmente in ambito finanziario, industriale e nella Pubblica Amministrazione.

La Società s'impegna a comprendere le esigenze dei clienti, per soddisfarle adeguatamente in conformità alle aspettative di qualità e di sicurezza. Nel gestire il patrimonio informativo affidatole dai Clienti, utilizzando metriche definite e misurabili.

Analogamente, la Società agisce nel rispetto delle necessità e dei requisiti di sicurezza che coinvolgono:

- il mercato di riferimento;
- il Sistema Paese in cui opera, rispettando le norme di riferimento vigenti;
- tutte le parti interessate (Dipendenti e Collaboratori, Fornitori, Partner, Autorità, etc.).

A dimostrazione dell'impegno per la gestione della sicurezza nella progettazione, sviluppo e manutenzione di software e nella fornitura/erogazione di servizi digitali, E-time ha realizzato e mantiene aggiornato un Sistema di Gestione per la Sicurezza delle Informazioni conforme alla norma internazionale ISO/IEC 27001:2022, estesa alle linee guida ISO/IEC 27017 ed ISO/IEC 27018 per i fornitori di infrastrutture e servizi cloud e per la protezione dei dati personali trattati in cloud pubblici.

5 SCOPO

L'organizzazione E-time considera obiettivo prioritario, salvaguardare la sicurezza del patrimonio informativo in gestione, tutelando la riservatezza, l'integrità e la disponibilità delle informazioni raccolte, elaborate, conservate o in qualunque modo trattate, da ogni minaccia intenzionale o accidentale, interna o esterna, avendo cura di valutare l'impatto del cambiamento climatico sulle proprie attività ed obiettivi strategici.

In tale contesto, il Sistema di Gestione per la Sicurezza delle Informazioni di E-time stabilisce e mantiene adeguate un set di misure di sicurezza inerenti gli aspetti organizzativi, relativi al personale, fisici e tecnologici, a garanzia del soddisfacimento di livelli adeguati delle caratteristiche di sicurezza di informazioni, sistemi e servizi:

- **Riservatezza**: l'informazione deve essere preservata da accessi impropri, ossia deve essere nota solo a chi è autorizzato;
- **Integrità**: l'informazione deve essere quella autentica anche a seguito di malfunzionamenti o danni dei sistemi e servizi, ossia l'informazione deve essere modificabile in modo legittimo e tracciabile solo ed esclusivamente da chi è autorizzato;
- **Disponibilità**: si applica sia alle informazioni che ai sistemi e servizi che le trattano ed è intesa come la salvaguardia del patrimonio informativo gestito nella sua garanzia di accesso e usabilità, riducendo furti, intrusioni e interruzioni.

L'organizzazione E-time è adeguata al Regolamento UE 2016/679 (GDPR) ed alla normativa nazionale (Codice Privacy) per la protezione dei dati personali, consolidando struttura organizzativa, personale e soluzioni tecnologiche e orientando le risorse per garantire Sicurezza e Privacy del patrimonio informativo gestito.

Per rispondere in modo ottimale alla protezione delle informazioni, E-time segue un approccio di gestione del rischio come base di riferimento della presente Politica di sicurezza, realizzando periodicamente una valutazione dei rischi inerenti il patrimonio informativo e gli asset di supporto che costituiscono il Sistema di Gestione delle Informazioni, al fine di comprendere le vulnerabilità a cui sono esposte, di valutare le possibili minacce che possono sfruttarle e di predisporre le necessarie contromisure, in linea con le indicazioni riportate nelle norme della famiglia ISO/IEC 27000 e le buone pratiche riconosciute dalla comunità di riferimento nazionale ed internazionale.

6 AMBITO DI APPLICAZIONE

La politica per la sicurezza delle informazioni di E-time si applica a tutto il personale interno ed alle terze parti che collaborano alla gestione delle informazioni trattate ed a tutti i processi, funzioni e risorse coinvolte nella progettazione, sviluppo, erogazione, manutenzione e assistenza di soluzioni software e servizi cloud.

Il software è progettato seguendo la metodologia Agile e sviluppata utilizzando tecnologie web e cloud computing.

Le applicazioni software vengono rese disponibili ai Clienti in due diverse modalità:

- come servizio in cloud (SaaS - Software as a Service), ospitato da un Fornitore riconosciuto affidabile (CISP - Cloud Infrastructure Service Provider) nel territorio nazionale ed UE;
- on-premises, installato presso l'infrastruttura fisica o virtualizzata del Cliente.

7 IMPEGNO DELLA DIREZIONE E CONTESTO ORGANIZZATIVO

La direzione di E-time considera la sicurezza del patrimonio informativo gestito uno strumento strategico per la soddisfazione del Cliente, del successo aziendale, un obiettivo da perseguire in tutte le attività dell'organizzazione.

Pertanto, s'impegna a promuovere una conoscenza ed un approccio condiviso in materia di sicurezza delle informazioni nonché ad esercitare la propria attività di governo responsabilmente e solidalmente con il contributo e la tutela dei suoi collaboratori e altre parti interessate.

Al fine di assicurare un'adeguata gestione della sicurezza, E-time è dotata di idonee strutture organizzative ed ha costituito un gruppo SGSI per l'identificazione e il controllo delle misure tecniche ed organizzative di prevenzione e protezione della riservatezza, dell'integrità e della disponibilità delle informazioni, tramite l'attuazione del Sistema di Gestione della Sicurezza delle Informazioni e con il contributo dei fornitori coinvolti, seguendo un approccio di responsabilità condivisa.

I sistemi infrastrutturali e gli applicativi esternalizzati sono monitorati da figure specialistiche interne, che hanno la responsabilità di assicurarsi che i

Fornitori di tecnologie operino in conformità agli accordi contrattuali, condizioni di fornitura di prodotti e servizi ed alla normativa di riferimento applicabile.

A tal fine, la Direzione ha destinato risorse (economiche, tecnologiche, organizzative e umane) necessarie alla realizzazione e mantenimento del Sistema di Gestione che sarà costantemente monitorato e periodicamente valutato, misurando il raggiungimento degli obiettivi fissati per i processi inclusi nel campo di applicazione, in cui effettuare la valutazione del rischio inerente alla sicurezza delle informazioni.

Tutto ciò premesso, la Direzione di E-time ha definito la presente "Politica per la Sicurezza delle Informazioni" impegnandosi a garantire che essa venga compresa, attuata, diffusa e sostenuta ad ogni livello aziendale, richiedendo a tutte le componenti aziendali coinvolte nell'ambito definito di farla propria e di impegnarsi per la sua completa attuazione e miglioramento.

La Direzione, si impegna altresì a garantire la diffusione della Politica al personale attraverso gli strumenti aziendali idonei e renderla agevolmente disponibile alle parti interessate.

Per ulteriori informazioni si rimanda alla documentazione adottata per la gestione della sicurezza delle informazioni, tenendo conto del livello di responsabilità stabilito dall'organizzazione aziendale.

8 Obiettivi

Gli obiettivi della Politica per la Sicurezza delle Informazioni che E-time intende perseguire con l'impegno della Direzione, sono:

- dimostrare alle parti interessate la propria capacità di fornire con regolarità servizi informatici sicuri, massimizzando gli obiettivi di sicurezza definiti;
- rispondere ai principi e ai controlli stabiliti dagli standard ISO/IEC 27001:2022 e ISO/IEC 27002:2022 e perseguire la conformità, in combinazione con altre linee guida e normative che disciplinano le attività in cui opera E-time, tra i quali, in particolare le regolamentazioni e linee guida ISO/IEC 27017 e ISO/IEC 27018, per l'impiego, l'implementazione ed erogazione dei servizi in cloud e la loro sicurezza e protezione delle informazioni, incluse quelle personali;

- garantire al personale e ai collaboratori un'adeguata conoscenza e grado di consapevolezza degli aspetti connessi con la sicurezza delle informazioni, al fine di consentire agli stessi di acquisire sufficiente coscienza della propria responsabilità durante le operazioni di trattamento;
- cogliere le opportunità che si possono verificare nel mantenimento e miglioramento del sistema di gestione per la Sicurezza delle Informazioni;
- affrontare e minimizzare il rischio di perdita e/o indisponibilità delle informazioni trattate, pianificando e gestendo le attività a garanzia della continuità di servizio, e gestione tempestiva di incidenti;;
- svolgere una continua e adeguata valutazione dei rischi che esamini costantemente le vulnerabilità e le minacce associate all'ambiente operativo a cui si applica il Sistema di gestione;
- rispettare le leggi e le disposizioni vigenti, i requisiti contrattuali e le procedure in essere;
- promuovere la collaborazione, comprensione e consapevolezza di SGSI da parte dei fornitori strategici;
- considerare l'adozione, con il contributo di Fornitori di tecnologie coinvolti, di misure che possono impattare sul cambiamento climatico connesse alla sicurezza delle informazioni.

E-time è regolarmente impegnata nella protezione dei dati personali dei soggetti interessati che gestisce, con particolare riferimento a quelli dei propri utenti fruitori di prodotti e servizi. Rispetto a questi ultimi l'organizzazione E-time, in accordo con la normativa privacy, nazionale ed europea, agisce come descritto nelle informative privacy in qualità di Titolare del trattamento. Tali obblighi sono riportati anche nelle nomine a Responsabile (ex art. 28 GDPR) dei Fornitori utilizzati dall'organizzazione E-time per svolgere il trattamento delle informazioni di carattere personale.

9 Comunicazione della Politica

La presente Politica è parte integrante di SGSI ed è divulgata a tutto il personale, ai collaboratori, ai clienti e ai fornitori attraverso il sito internet istituzionale o altra modalità adatta stabilita dalla Direzione.

I vertici aziendali, il personale dipendente, e alcuni soggetti esterni identificati nel SGSI sono tenuti a rispettare questa Politica e il Sistema di Gestione che la implementa, contribuendo al mantenimento ed al miglioramento continuo.

Il gruppo SGSI attraverso opportune sessioni informative e formative sensibilizza gli utenti interni ad una corretta applicazione delle procedure operative che riguardano la sicurezza delle informazioni, stimolando gli stessi a collaborare fattivamente per una gestione sempre più coordinata ed esaustiva di tale tematica.

Tutto il personale, nel contesto delle proprie responsabilità e consapevolezza, è coinvolto nella segnalazione al gruppo SGSI eventi di pericolo, incidenti potenziali o manifestati e di qualsiasi vulnerabilità/debolezza e danneggiamento definito o che potrebbe coinvolgere il Sistema di Gestione.

Le conseguenze della violazione della presente Politica sono stabilite nel documento di Regolamento disciplinare interno all'organizzazione, nei contratti e negli accordi con terze parti.

10 Riesame della politica

Il presente documento è di proprietà di E-time srl ed è responsabilità della Direzione, in collaborazione con il gruppo SGSI, provvedere all'aggiornamento puntuale del medesimo, affinché la politica descritta ed implementata da SGSI sia allineata a fenomeni di cambiamento ed evoluzione che coinvolgono la protezione delle informazioni.

E-time è consapevole che il riesame periodico e regolare della presente politica di sicurezza è conseguente al verificarsi di incidenti relativi alla sicurezza, alla continua evoluzione tecnologica ed al condizionamento normativo, così come a cambiamenti organizzativi. Tutto ciò porta alla nascita di nuove problematiche di sicurezza che potrebbero incidere sulla capacità di mantenere gli obiettivi di sicurezza stabiliti o portare alla modifica del livello di sicurezza complessivo.

A titolo esemplificativo, si riportano alcune delle principali dimensioni che sono motivo di riesame:

- aggiornate le strategie organizzative e gli obiettivi strategici aziendali;
- introdotte modifiche funzionali e tecnologiche con impatti sulla sicurezza delle informazioni;
- rivalutate le politiche di sicurezza delle parti coinvolte;
- adeguamenti a standard di riferimento e normative vigenti.

San Martino Buon Albergo, 15 aprile 2024

La Direzione di E-time