INERA srl
Via G.Malasoma, 18
56121 Pisa

Tel. 050 9911800 – Fax 050 9911830
Registro delle Imprese di Pisa N. 01558430508 R.E.A. 136540
P.I. e C.F. 01558430508
Capitale Sociale Euro 200.000 i.v.

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

LISTA DI DISTRIBUZIONE	
Sito Internet	www.inera.it
Personale Inera	Archivio condiviso
Gruppo SGS	Cartella Qualità
Qualità	Cartella Qualità
Direzione	Cartella Qualità

Emesso e verificato dal RQ	05.09.2022
Approvato dalla Direzione	06.09.2022

INERA srl
Via G.Malasoma, 18
56121 Pisa

Tel. 050 9911800 – Fax 050 9911830
Registro delle Imprese di Pisa N. 01558430508 R.E.A. 136540
P.I. e C.F. 01558430508
Capitale Sociale Euro 200.000 i.v.

INDICE

1 PREMESSA GENERALE

Inera è un'azienda ultraventennale specializzata nell'ICT che fornisce strumenti e tecnologie a supporto della comunicazione digitale con un'offerta specializzata e di alto profilo.

Le principali aree di interesse sono:

- Siti e Portali Web.
- Catalogazione, Pubblicazione ed Accesso a Banche Dati on-line.
- Creazione e gestione di archivi digitali.
- Commercio Elettronico.
- Applicazioni Web e Mobile.
- Architetture di Sistemi e di Rete.
- Analisi del visuale e Realtà aumentata.
- Open Source.

Il core business di INERA sono principalmente le pubbliche amministrazioni, sia centrali che locali. I settori di mercato in cui opera sono essenzialmente i seguenti: Beni Culturali, Turismo, Stampa e editoria online.

L'obiettivo di Inera è di proporre ai propri clienti prodotti e soluzioni avanzate basati su tecnologie Internet con particolare cura delle problematiche di integrazione di diverse tecnologie e degli strumenti di supporto alla manutenzione e gestione delle applicazioni realizzate.

2 IMPEGNO DELLA DIREZIONE E SCOPI

L'azienda, già certificata di qualità con la norma UNI EN ISO 9001: 2015 per "Progettazione, sviluppo, installazione e assistenza di prodotti e soluzioni software", ha deciso di istituire un Sistema di Gestione per la Sicurezza delle Informazioni in conformità alla norma EN ISO/IEC 27001:2013 per garantire e proteggere i dati e le informazioni dalle possibili minacce, attraverso un processo continuo di gestione dei rischi.

In particolare, gli scopi del SGSI sono i seguenti:

- avere una visione complessiva e centrale della sicurezza aziendale che spazia oltre il perimetro della sicurezza IT includendo anche persone e processi secondo un approccio olistico;
- disporre di strumento fondamentale per l'ottimizzazione dell'allocazione del budget indirizzandolo verso le iniziative che restituiscono un maggior ritorno in termini di riduzione del rischio;
- dimostrare la sua abilità nel fornire e servizi conformi ai requisiti dei clienti, ai requisiti degli standard di riferimento, delle leggi e dei regolamenti applicabili;
- incrementare la soddisfazione dei clienti attraverso l'efficace applicazione del SGSI e dei processi di miglioramento continuo e assicurando il rispetto dei requisiti stabiliti dalle normative cogenti e dai regolamenti applicabili.

3 DICHIARAZIONE SULLA POLITICA AZIENDALE PER LA SICUREZZA DELLE INFORMAZIONI

Essere competitivi significa puntare a differenziare le caratteristiche dei propri servizi attraverso una costante ricerca volta al miglioramento dei processi aziendali dai punti di vista della qualità, delle prestazioni aziendali e della sicurezza delle informazioni.

Inera ritiene che la sicurezza delle informazioni rappresenti un fattore critico di successo sia per quanto riguarda i processi di progettazione e sviluppo di soluzioni tecnologiche che per quanto riguarda l'erogazione dei servizi.

Per Inera la Gestione della Sicurezza delle Informazioni ha come obiettivo primario la protezione dei dati e delle informazioni al fine di tutelare il patrimonio rappresentato dalle conoscenze aziendali, quello dei propri clienti e di tutelare le persone fisiche di cui si trattano i dati personali.

Per le caratteristiche dei servizi che Inera offre ai propri clienti e per il valore che rappresentano le informazioni nel proprio business la Politica della Sicurezza delle Informazioni rappresenta un indirizzo strategico fondamentale e prioritario.

La Politica della Sicurezza delle Informazioni definisce e organizza la riservatezza delle informazioni, l'integrità informatica e gestisce tutti gli aspetti ad essa collegati, da quelli tecnici a quelli di management e di business, incluse la confidenzialità e disponibilità dei dati.

La politica per la sicurezza delle informazioni per Inera è costituita da un insieme di attività che comprendono: l'identificazione delle aree critiche, la gestione dei rischi, dei sistemi e della rete, delle vulnerabilità e degli incidenti, il controllo degli accessi, la gestione della privacy e della compliance, la valutazione dei danni e tutti gli altri aspetti che possono impattare sulla gestione della sicurezza delle informazioni.

Per perseguire questo obiettivo Inera, attraverso un approccio by design, pone grande attenzione alla progettazione, alla gestione e alla manutenzione della propria struttura tecnologica, fisica, logica ed organizzativa.

Inera impegna quindi la propria organizzazione e specificatamente le proprie persone a sviluppare e manutenere un Sistema di Gestione della Sicurezza delle Informazioni nell'ambito delle attività svolte e dei servizi erogati al fine di garantire la disponibilità l'integrità e la riservatezza dei dati, oltre che delle informazioni e degli accessi.

Tutte le persone che lavorano e/o collaborano con Inera sono impegnate a rispettare i seguenti principi:

1. Riservatezza: per assicurare che l'informazione sia accessibile solamente ai soggetti e/o ai processi debitamente autorizzati e che le informazioni non siano rese disponibili o divulgate a persone o entità non autorizzate;
2. Integrità: per salvaguardare la consistenza dell'informazione da modifiche non autorizzate e garantire che l'informazione non subisca modifiche o cancellazioni a seguito di errori o di azioni volontarie, ma anche a seguito di malfunzionamenti o danni dei sistemi tecnologici;
3. Disponibilità: per assicurare che gli utenti autorizzati abbiano accesso alle informazioni e agli elementi architetturali associati quando ne fanno richiesta e salvaguardia quindi il patrimonio informativo nella garanzia di accesso, usabilità e

confidenzialità dei dati, riducendo i rischi connessi all'accesso alle informazioni (intrusioni, furto di dati, ecc.);
4. Controllo: per assicurare che la gestione dei dati avvenga sempre attraverso processi e strumenti sicuri e testati;
5. Privacy: per garantire la protezione ed il controllo dei dati personali.

La Direzione è fortemente impegnata a una grande responsabilizzazione di tutte le persone che lavorano per e con Inera nel garantire la rigorosità del proprio operato per adempiere, con la massima attenzione, ai compiti assegnati. In particolare, questo obiettivo è perseguito attraverso l'impegno a garantire:

- il rispetto delle leggi e normative vigenti;
- l'efficienza operativa e affidabilità dei processi di sviluppo prodotti e servizi correlati;
- le condizioni di salute e sicurezza sui luoghi di lavoro per il personale e terzi;
- la continuità e l'efficienza dei processi organizzativi e operativi al fine di prevenire e ridurre al minimo l'impatto degli incidenti volontari o casuali sulla sicurezza dei dati/informazioni gestite;
- la protezione dei mezzi resi disponibili, ed il loro corretto utilizzo;
- la riservatezza, la correttezza e la disponibilità dei dati/informazioni gestiti da Inera e la salvaguardia della proprietà intellettuale;
- l'adozione di misure di prevenzione di anomalie di processo/prodotto/servizio.

4 IL SISTEMA DI GESTIONE DELLA SICUREZZA DELLA INFORMAZIONI | SGSI

Per dare attuazione alla propria politica della sicurezza delle informazioni, **Inera, ha sviluppato e si impegna a mantenere un sistema di gestione sicura delle informazioni conforme ai requisiti specificati delle norme UNI CEI EN ISO/IEC 27001:2013** e delle leggi cogenti come mezzo per gestire la sicurezza delle informazioni nell'ambito della propria attività.

Nell'ambito della gestione dei servizi offerti, Inera assicura:

1. l'osservanza dei livelli di sicurezza stabiliti attraverso l'implementazione SGSI (sistema di gestione della sicurezza delle informazioni)
2. il rispetto delle normative vigenti e degli standard internazionali di sicurezza per la propria infrastruttura tecnologica e organizzativa
3. fornisce la garanzia di selezionare fornitori e partner affidabili dal punto di vista della gestione in sicurezza delle informazioni e della protezione dei dati personali.

La politica per la sicurezza delle informazioni di Inera si applica a tutto il personale interno e quello delle terze parti che collaborano alla gestione delle informazioni ed a tutti i processi e risorse coinvolte nella progettazione, realizzazione, avviamento ed erogazione continuativa nell'ambito dei servizi.

La politica della sicurezza di Inera rappresenta in concreto l'impegno dell'organizzazione nei confronti di clienti e delle terze parti a garantire la sicurezza delle informazioni, degli strumenti fisici, logici e organizzativi atti al trattamento delle informazioni in tutte le attività.

In sintesi, la politica della sicurezza delle informazioni di Inera garantisce che:

- l'organizzazione abbia piena conoscenza delle informazioni gestite e valuti di volta in volta la loro criticità, al fine di agevolare l'implementazione di adeguati livelli di protezione;
- l'accesso alle informazioni avvenga in modo sicuro e adatto a prevenire i trattamenti non autorizzati o realizzati senza i diritti necessari;
- l'organizzazione e le terze parti collaborino al trattamento delle informazioni adottando procedure volte al rispetto di adeguati livelli di sicurezza;
- l'organizzazione e le terze parti che collaborano al trattamento delle informazioni siano adeguatamente formate e abbiano piena consapevolezza delle problematiche relative alla sicurezza;
- le anomalie e gli incidenti aventi ripercussioni sul sistema informativo, sui servizi e sui livelli di sicurezza aziendale siano tempestivamente riconosciuti e correttamente gestiti attraverso efficienti sistemi di prevenzione, comunicazione e reazione al fine di minimizzare l'impatto sul business;
- l'accesso alla sede ed ai singoli locali aziendali avvenga esclusivamente da personale autorizzato, a garanzia della sicurezza delle aree e degli asset presenti;
- la conformità con i requisiti di legge ed il rispetto degli impegni di sicurezza stabiliti nei contratti con le terze parti;
- la rilevazione di eventi anomali, incidenti e vulnerabilità dei sistemi informativi al fine di rispettare la sicurezza e la disponibilità dei servizi e delle informazioni;
- la business continuity aziendale e il disaster recovery, attraverso l'applicazione di procedure di sicurezza stabilite;
- i trattamenti dei dati personali, sia nei casi in cui Inera operi in qualità di Titolare che nei casi in cui operi per conto terzi in qualità di Responsabile del Trattamento, avvenga nel rispetto del Regolamento Europeo sulla Protezione dei Dati Personali GDPR 679/2016.

La politica della sicurezza delle informazioni viene costantemente aggiornata e verificata, attraverso un riesame semestrale, per assicurare il suo continuo miglioramento ed è condivisa con l'organizzazione, le terze parti ed i clienti, attraverso la sua pubblicazione sul sito.

5 DICHIARAZIONE DI IMPEGNO

Inera si impegna a garantire:

- **la riservatezza delle informazioni** attraverso la definizione puntuale delle responsabilità interne per la gestione dei servizi e delle informazioni ad essi connesse; il controllo degli accessi fisici e logici agli archivi elettronici e cartacei esclusivamente da parte di personale autorizzato e competente;
- **l'integrità delle informazioni** attraverso il controllo degli accessi fisici e logici agli archivi elettronici esclusivamente da parte di personale autorizzato e competente e la gestione dei back-up dei dati e delle configurazioni dei sistemi informativi;
- **la disponibilità delle informazioni** attraverso l'identificazione dei ruoli e delle funzioni, i diritti di accesso alle informazioni e agli assets aziendali per la gestione dei servizi al Cliente;
- che dipendenti, fornitori, partner, appaltatori e ogni altra terza parte coinvolta con il trattamento di informazioni che rientrano nel campo di applicazione del Sistema di Gestione della Sicurezza delle Informazioni, accettino **gli obblighi e le**

responsabilità di propria pertinenza, al fine di proteggere le informazioni, i beni e le risorse di Inera;

- che ogni **accesso**, di tipo fisico o informatico, sia autorizzato, **controllato** e monitorato sulla base dei seguenti criteri: (a) l'accesso è autorizzato al personale abilitato solo per le informazioni necessarie (principio della conoscenza minima o necessità di sapere); (b) l'accesso è autorizzato al personale abilitato solo per le informazioni relative alle attività specifiche (funzione di lavoro-correlati); (c) l'accesso alla struttura e ai locali è autorizzato al personale abilitato. L'accesso ai locali di Inera è autorizzato, controllato e monitorato in linea con la politica aziendale.
- che ogni dipendente, fornitore, imprenditore e terza parte sia **consapevole** del proprio ruolo e dell'impatto delle proprie azioni sulla sicurezza delle informazioni.
- che ogni risorsa sia adeguatamente **formata** e addestrata sulle politiche e sulle procedure relative alla gestione della sicurezza delle informazioni.
- che i trattamenti delle informazioni, delle attività, delle risorse e delle soluzioni inerenti la protezione delle informazioni di Inera o gestiti dalla stessa per conto dei propri clienti sono **conformi alle leggi e ai regolamenti** applicabili di natura cogente, contrattuale e volontaria.
- che ogni attività e risorsa di Inera o affidata da questa a terze parti, nonché ogni informazione pertinente l'ambito del SGSI, è **protetta** contro i problemi legati alla riservatezza, l'integrità e la disponibilità, in proporzione al loro valore e nel rispetto delle leggi vigenti.
- che tutto il **personale** Inera sia **responsabilizzato** all'obbligo di: (a) garantire il rispetto delle norme, leggi e regolamenti vigenti, di natura cogente, contrattuale e volontaria rese applicabili negli ambiti del SGSI; (b) proteggere la riservatezza, l'integrità e la disponibilità delle informazioni gestite da Inera, la proprietà intellettuale e il patrimonio di Inera o da questa affidati a terze parti; (c) aver cura dei beni materiali, i sistemi e le risorse di Inera; (d) salvaguardare e gestire in modo appropriato ogni informazione e dato afferenti le attività di propria competenza; (e) contattare la Direzione, il Responsabile della Sicurezza delle informazioni e/o altre autorità competenti in caso di effettive o sospette violazioni della sicurezza; (f) segnalare qualsiasi necessità di modifiche alle procedure relative alla gestione della sicurezza delle informazioni. Compatibilmente con le autorità assegnate nella gestione della sicurezza ciascuno deve: (g) garantire la conformità con la politica di sicurezza, requisiti, standard e/o procedure definiti; (h) individuare e definire i diritti di accesso agli assets per le loro specifiche attività e responsabilità; (i) richiedere alle terze parti di essere formalmente in linea con gli accordi di riservatezza; (l) operare in conformità ai livelli di rischio che sono stati definiti per il proprio ambito di pertinenza.
- che tutto il **personale** cui sono assegnate responsabilità specifiche nella gestione della sicurezza delle informazioni **ha** altresì il **dovere** di: (m) implementare la sicurezza sulla base delle politiche di sicurezza della Inera; (n) garantire e monitorare il rispetto delle politiche di sicurezza delle informazioni, requisiti, norme e procedure definiti da Inera nell'ambito del SGSI; (o) monitorare gli assets aziendali, al fine di garantire il rispetto del livello di controllo previsto per l'asset da proteggere ed il rispetto delle leggi e regolamenti applicabili; (p) rendere effettive l'insieme di regole, funzioni, strumenti, oggetti e controlli, resi coerenti e funzionali agli scopi dell'organizzazione e coerenti con gli ambiti del SGSI, che garantiscano che nella struttura, organizzazione, ambiente informatico, singolo elaboratore, sia

costantemente osservato il rispetto dei requisiti del SGSI; (q) garantire che il personale di Inera e i terzi siano formati e informati circa la politica, i requisiti, standard e/o procedure per la gestione della sicurezza delle informazioni, nonché resi consapevoli delle conseguenze in caso di mancato rispetto della politica e requisiti stabiliti in tali ambiti; (r) sostenere l'adozione di misure adeguate a garantire il controllo sugli aspetti che hanno impatto sulla sicurezza delle informazioni; (s) contenere il livello di rischio negli ambiti di pertinenza; (t) mantenere attive le misure da adottarsi in caso di incidenti derivanti dal verificarsi di condizioni anomale e di emergenza, garantire l'adozione dei piani di continuità in conformità ai requisiti definiti dal SGSI.

- Inoltre, che i **soggetti terzi** che gestiscono in modo diretto o indiretto gli assets sensibili di Inera e dei Clienti, **sono obbligati**, nello svolgimento di processi/attività, a: (u) formalizzare il proprio impegno alla riservatezza e non divulgazione delle informazioni tratte negli ambiti di competenza; (v) proteggere le risorse e le informazioni fisiche e intellettuali a cui possono accedere nella effettuazione delle attività assegnate; (z) garantire la piena osservanza ai requisiti del SGSI nei comportamenti e nell'operatività.

In conclusione, Inera si impegna a:

- **adottare un sistema di gestione sicura delle informazioni conforme ai requisiti specificati delle Norme UNI CEI EN ISO/IEC 27001:2013**
- **mantenere costantemente monitorato il grado di conformità del sistema alle norme e leggi applicabili di natura cogente e volontaria, e gli obblighi contrattuali pertinenti l'ambito di applicazione del SGSI;**
- **garantire mezzi e risorse idonee al suo mantenimento e miglioramento continuo, in particolare per quanto attiene la mitigazione/riduzione dei livelli di rischio sulla sicurezza delle informazioni e l'adozione di misure idonee a prevenire – ovvero gestire adeguatamente – situazioni anomale e di emergenza;**
- **rendere consapevoli tutte le persone che dell'organizzazione degli obblighi e delle responsabilità di ciascuno nella gestione della sicurezza delle informazioni e delle conseguenze in caso di eventi, dolosi e colposi, relativi all'utilizzazione non autorizzata, modifica o distruzione di informazioni critiche.**