ALL. 3.B	
Titolo : **POLITICA SGSI E DEFINIZIONE DEGLI OBIETTIVI**	

MANIFESTO POLITICA SGSI

Il Managment della **FATA INFORMATICA SRL** ha definito una **Politica sulla sicurezza** al fine di:

- Assicurare la selezione e adozione di controlli al fine di proteggere le informazioni e gli asset
- Minimizzare i rischi di business globali e di sicurezza e dare fiducia alle parti interessate
- Perseguire il miglioramento continuo della sicurezza delle informazioni

Su tale linea FATA INFORMATICA ha deciso di porre in essere un Sistema di Gestione per la Sicurezza delle Informazioni definito secondo regole e criteri previsti dalle "best practice" e dagli standard internazionali di riferimento in conformità anche alle indicazioni della norma internazionale ISO IEC 27001:2013 e delle Linee Guida ISO/IEC 27017:2015 – ISO/IEC 27018:2019;

Con la presente Politica la FATA INFORMATICA intende inoltre:

- Proteggere il proprio patrimonio informativo
- Adottare le misure atte a garantire la fidelizzazione del personale e la sua professionalizzazione
- Rispondere pienamente alle indicazioni della normativa vigente e cogente;
- Aumentare, nel proprio personale, il livello di sensibilità e la competenza su temi di sicurezza.

La direzione della FATA INFORMATICA si impegna quindi a:

- predisporre tutte le azioni necessarie per perseguire obiettivi di sicurezza congrui al grado di sensibilità delle Informazioni aziendali e di criticità delle tecnologie che consentono il loro trattamento, garantendo:
    - riservatezza delle informazioni mediante interventi idonei a contrastare accessi non autorizzati alle informazioni o diffusione o divulgazione non controllate delle stesse;
    - integrità delle informazioni mediante interventi idonei a contrastare il verificarsi di modifiche non autorizzate, compresi gli errori umani o il danneggiamento del formato fisico e/o del contenuto semantico delle informazioni;
    - disponibilità delle informazioni mediante interventi idonei a garantire l'accesso alle risorse informative con tempi e modalità "congrue" alle esigenze delle attività di business;
- cooperare con i Clienti al fine di accrescere il livello di sicurezza delle informazioni dei loro sistemi e processi;
- effettuare sistematicamente attività di analisi e gestione dei rischi impattanti sulla sicurezza delle informazioni, in conformità alle policy ed ai modelli aziendali alle direttive per la protezione dei dati personal, per identificare i controlli necessari da adottare anche in riferimento al continuo evolversi del quadro esterno di minacce (cybersecurity);
- monitorare a livello aziendale lo stato della sicurezza delle informazioni e dei sistemi ICT e il livello di compliance al quadro regolamentare interno nonché contrattuale ed agli eventuali vincoli normativi anche in materia di protezione dei dati personali;
- assicurare un costante miglioramento delle misure di sicurezza adottate per la protezione dei dati personali dei clienti e delle parti interessate nella gestione aziendale e nell'erogazione dei servizi (on premise e in cloud);
- prevenire e gestire gli eventi e/o gli incidenti di sicurezza delle informazioni e/o violazione dei dati personali, raccogliendo e conservando le relative registrazioni:
- promuovere ed attuare piani mirati o diffusi di formazione e sensibilizzazione sulla sicurezza delle informazioni.

OBIETTIVI

La FATA INFORMATICA al fine di garantire determinati livelli di **confidenzialità, integrità e disponibilità** delle informazioni sia interne sia affidate dai clienti, di adotta le seguenti misure tecniche, organizzative riportate nelle procedure del SGSI:

- Requisiti della sicurezza delle informazioni
- Classificazione dei beni
- Analisi e valutazione dei rischi
- Misure di protezione previste in conformità alla normativa vigente
- Misure di protezione fisica ed ambientale
- Misure di protezione logica
- Misure di sicurezza organizzativa
- Business continuity
- Incidenti di sicurezza
- Monitoraggio delle misure di sicurezza
- Audit delle misure di sicurezza
- Controllo delle eventuali situazioni di outsourcing
- Controllo dei servizi gestiti tramite piattaforme cloud
- Aggiornamento e manutenzione delle misure di sicurezza
- Piano di comunicazione, sensibilizzazione e formazione
- Verifiche tecniche di sicurezza tramite vulnerability assessment e penetration test periodici nelle infrastrutture e negli applicativi per valutare la resilienza dei sistemi ad attacchi esterni ed evincere eventuali vulnerabilità e consentirne il successivo fixing.

Per quel che riguarda invece le attività comprese nello scopo di certificazione i livelli di sicurezza stabiliti per i criteri di **riservatezza (R), integrità (I) e disponibilità (D)** delle informazioni sono i seguenti:

	Sviluppo	Gestione e manutenzione	Vulnerability Assessment	Gestione servizi Cloud
Riservatezza Garantire che l'informazione sia accessibile soltanto ai soggetti autorizzati	• rigorosa separazione dell'ambiente di sviluppo da quelli di collaudo ed esercizio • identificazione, autorizzazione degli utenti e degli accessi • confidenzialità dei processi e della documentazione di sviluppo • formazione e sensibilizzazione del personale	• identificazione e autorizzazione del personale deputato ad operare nei contesti di intervento • confidenzialità dei dossier di intervento e delle casistiche e/o problematiche riscontrate presso il cliente	• consapevolezza sui rischi di sicurezza, conseguente a specifica formazione e/o addestramento, del personale coinvolto nell'intervento • verifica robustezza accessi non autorizzati • identificazione, autorizzazione e registrazione del personale deputato all'intervento • rispetto rigoroso dei limiti fisici, logici e sociali dell'intervento	• identificazione e autorizzazione del personale deputato ad operare sui dati dei clienti • confidenzialità sulla gestione dei dati degli utenti dei servizi • gestione accordi di riservatezza e contrattuali con il cloud service provider di infrastruttura • gestione accordi contrattuali standard con i clienti per il cloud • formazione e sensibilizzazione del personale • conformità con le policy, corporate e/o di governo, specifiche dell'ambiente cloud e in materia di dati personali
Integrità Garantire l'accuratezza e la completezza dell'informazione e delle relative	• conservazione dei software e dei documenti di progetto in dei repository SVN	• formazione e sensibilizzazione del personale per minimizzare l'impatto di possibili cambiamenti o	• compliance con requisiti legali, operativi e contrattuali che regolano l'assessment	• gestione accordi contrattuali e di servizio con il cloud service provider di infrastruttura

procedure		incidenti correlati a servizi IT • conformità con le policy, corporate e/o di governo, specifiche dell'ambiente in cui si va a operare	• best practices per prevenire la perdita dei dati	• formazione e sensibilizzazione del personale per minimizzare l'impatto di possibili cambiamenti o incidenti correlati a servizi IT • conformità con le policy, corporate e/o di governo, specifiche dell'ambiente cloud e in materia di dati personali
Disponibilità Garantire che gli utenti autorizzati abbiano accesso all'informazione e agli asset associati ogni volta che sia necessario	• best practices di system resiliency • redazione di policy e procedure di backup e restore dei repository SVN e degli ambienti di sviluppo	• formazione e sensibilizzazione del personale per minimizzare l'impatto di possibili cambiamenti o incidenti correlati a servizi IT • rispetto di tempi e modalità di intervento, concordati con il cliente • redazione di policy e procedure di incident handling	• preservazione dell'ambiente durante l'intervento quando possibile.	• gestione accordi contrattuali e di servizio con il cloud service provider di infrastruttura • formazione e sensibilizzazione del personale per minimizzare l'impatto di possibili cambiamenti o incidenti correlati a servizi IT • best practices di system resiliency • rispetto di SLA sulla disponibilità dei servizi

Infine lo staff operativo della FATA INFORMATICA si attiene ad alcune Linee Guida interne (Best Practices) per quel che riguarda:

- Linea guida 01 per la Sicurezza informatica (progettazione, sviluppo e test)
- Linea guida 02 per la Sicurezza informatica (gestione delle postazioni client)
- Linea guida 03 per la Sicurezza informatica (gestione dei servizi cloud)

E' stato predisposto un corso di Cyber Security Awareness per tutti i dipendenti.
Sono state definite le informazioni necessarie per lo smart working e condiviso con i dipendenti.

RESPONSABILITA'

TUTTO IL PERSONALE è responsabile dell'osservanza di questa policy e della segnalazione di anomalie di cui dovesse venire a conoscenza.

TUTTI I SOGGETTI ESTERNI che, intrattengono rapporti con la FATA INFORMATICA devono garantire il rispetto dei requisiti di sicurezza esplicitati dalla presente politica di sicurezza anche attraverso la sottoscrizione di un "Accordo di riservatezza" all'atto del conferimento dell'incarico allorquando questo tipo di vincolo non sia espressamente citato nel contratto.

RIESAME

FATA INFORMATICA verificherà periodicamente l'efficacia e l'efficienza del SGSI, garantendo l'adeguato supporto per l'adozione delle necessarie migliorie al fine di consentire l'attivazione di un processo continuo, che deve tenere sotto controllo il variare delle condizioni al contorno o degli obiettivi di business aziendali al fine di garantire il suo corretto adeguamento.

DATA

13/01/2025

Firma Direzione

ALL. 3.A.	
Titolo : **DICHIARAZIONE DEGLI OBIETTIVI SGSI**	

A tal fine la Direzione di **FATA INFORMATICA Srl** è impegnata, per l'anno di riferimento 2023, nel raggiungimento dei seguenti obiettivi:

OBIETTIVI (AREA)	INDICATORE	PROCESS OWNER	RISORSE FINANZIARIE	TEMPI	PIANI DI MIGLIORAMENTO/ STRATEGIE	STEP DI MONITORAGGIO
RISK ANALYSIS **Presa in carico delle vulnerabilità del SGSI = Livello Medio (28:40) emerse nella RISK (Target: Livello rischi < Medio)**	Livello rischi = 28:40 RISK	ISM	/	1 anno	Definite all'interno del RISK TREATMENT PLAN M-I-A20 11.04.2023	Traguardi definiti all'interno del RISK TREATMENT PLAN M-I-A20
CONTINUITA' OPERATIVA **Aggiornare ove opportuno la mappa degli episodi avversi del BCP in relazione agli incident occorsi soprattutto di tipo logico ed evidenziati nel file M-I-23**	N. eventi aggiunti/tot eventi accaduti	ISM	/	1 anno	Valutando le azioni intraprese per la risoluzione degli stessi al fine di garantire la continuità operativa	Monitoraggio mensile del report M-I-23 per annotare eventi occorsi
FORMAZIONE DEL PERSONALE **Continuare nella erogazione della formazione delle risorse umane sui temi della sicurezza del sistema gestione delle informazioni (Target: almeno 20 ore nell'anno)**	n. ore formazione su SGSI presenti in AZIMUT/totale ore pianificate	ISM	1500 €	1 anno	Incarico a consulenti esperti per eseguire sessioni di formazione	Monitoraggio semestrale del piano di formazione

Ciò comporterà una costante applicazione da parte di tutti noi; direzione e dipendenti.

LA DIREZIONE GENERALE

Roma, emissione addì _09/01/2017_
Aggiornamento _15/09/2017_
Aggiornamento _ 01/10/2018_
Aggiornamento _ 30/08/2019_
Aggiornamento _ 30/08/2019_
Aggiornamento _ 19/04/2021_
Aggiornamento _ 20/04/2022
Aggiornamento _ 11/04/2023

_____