LA POLITICA AZIENDALE

HOST S.p.A., consapevole dell'importanza della qualità dei prodotti e dei servizi erogati nonché della protezione, riservatezza, integrità e disponibilità degli asset informativi dell'Organizzazione, ha implementato un sistema di gestione per la Qualità e per la Sicurezza delle Informazioni in accordo alle norme UNI EN ISO 9001:2015, UNI CEI EN ISO/IEC 27001:2017, UNI CEI EN ISO/IEC 27017:2015 e UNI CEI EN ISO/IEC 27018:2019 nella convinzione che il riconoscimento internazionale di tali standard rappresenti un elemento di garanzia, altresì, ha lo scopo di perseguire la soddisfazione delle parti interessate intese come tutti i soggetti portatori di interesse diretto o indiretto alle attività dell'Organizzazione.

Al fine di perimetrare, mettere in atto e migliorare il proprio sistema di gestione integrato, HOST S.p.A. ha analizzato e considerato le variabili del proprio contesto, classificato le parti interessate e le loro esigenze ed ha individuato i rischi strategici e le opportunità di sistema.

Nel definire la presente Politica la Direzione si impegna affinché essa sia appropriata agli scopi dell'Organizzazione e consenta effettivamente il miglioramento continuo dell'efficacia e dell'efficienza dei processi ed il rispetto delle prescrizioni legali applicabili.

SCOPI E OBIETTIVI

La Direzione di HOST S.p.A. ha definito, ha divulgato e si impegna a mantenere attiva a tutti i livelli della propria Organizzazione la presente politica per la Gestione della Qualità e della Sicurezza delle Informazioni.

Lo scopo della presente politica è garantire la massima soddisfazione del cliente nella fruizione dei nostri servizi e la tutela e la protezione da tutte le minacce, interne o esterne, intenzionali o accidentali, delle informazioni nell'ambito delle nostre attività in accordo con le indicazioni fornite dallo standard UNI CEI EN ISO/IEC 27001:2017 e dalle linee guida contenute nello standard UNI CEI EN ISO/IEC 27017:2015 e UNI CEI EN ISO/IEC 27018:2019, nelle loro ultime versioni.

Pertanto, **HOST S.p.A.** si impegna a raggiungere i seguenti obiettivi coerenti con la presente politica:

- **soddisfare le attese dei committenti e dei dipendenti** attraverso un processo di miglioramento continuo al quale partecipi ogni persona che lavora per l'Azienda, perseguendo un approccio proattivo allo scopo di evitare gli errori nell'erogazione dei servizi;
- **rispettare le leggi e i regolamenti pertinenti e la legislazione vigente** ed operare nel totale rispetto di quella che è la giurisprudenza, i regolamenti e le direttive sia a carattere nazionale che comunitario;
- **formulare obiettivi di miglioramento continuo** delle prestazioni in relazione alla qualità e alla sicurezza delle informazioni;
- **promuovere attività di formazione, informazione e sensibilizzazione**, coinvolgendo tutto il personale aziendale rendendolo consapevole dei suoi obblighi individuali e dell'importanza di ogni sua singola azione per il raggiungimento dei risultati attesi e della sua responsabilità in materia di qualità e sicurezza delle informazioni;
- **comunicare con le parti interessate e coinvolgerle**, attivando appropriati canali di comunicazione al proprio interno, tesi ad assicurare un continuo e proficuo scambio con tutto il personale e verso l'esterno;
- **garantire la sicurezza delle informazioni e i dati dei nostri clienti** che, in quanto beni aziendali, hanno un valore per l'Organizzazione, in modo da assicurare la continuità del business aziendale, minimizzare i danni e massimizzare il ritorno degli investimenti e delle opportunità commerciali;
- **adottare le misure tecniche e organizzative volte ad assicurare la salvaguardia della riservatezza, integrità e disponibilità delle informazioni gestite;**

- **proteggere la sicurezza dei sistemi** riducendo ad un valore accettabile la probabilità che vengano violati i parametri di sicurezza informatica, individuando tempestivamente quando ed in quale parte del sistema questo accade, limitando i danni e ripristinando i requisiti violati nel minor tempo possibile;
- **mantenere un alto livello professionale dei dipendenti**, collaboratori, professionisti perché questo è propedeutico al raggiungimento degli altri obiettivi: uniformandosi le tecnologie, è il fattore umano l'aspetto differenziale;
- **diffondere la cultura informatica** al fine di creare e promuovere un patrimonio di conoscenze e competenze che contribuiscano in modo sostanziale alla formazione di una coscienza e di un'identità informatica nel territorio, attraverso diverse metodologie di servizi e strumenti;
- **proteggere le risorse informatiche aziendali** attraverso la selezione e l'applicazione di appropriate misure precauzionali, che non devono essere percepite come vincoli e costrizioni alla missione dell'Organizzazione, ma come elementi che contribuiscono al raggiungimento degli obiettivi aziendali;
- **invogliare i fornitori** ad adottare un adeguato sistema di gestione qualità e sicurezza delle informazioni.
- **sensibilizzare le risorse interne ed esterne** al continuo rispetto delle procedure previste dal Protocollo condiviso al fine di contenere il più possibile il rischio di contagio da Covid-19.

Tutto quanto sopra descritto permette a **HOST S.p.A**. di continuare a distinguersi come fabbricatore di servizi innovando il mercato dell'hosting e impegnandosi a **pensare, progettare e realizzare vere e proprie residenze virtuali** per i propri clienti, restando sempre un passo avanti a livello di **sicurezza e innovazione** con **l'obiettivo** di **garantire la presenza online dei siti web, sempre.**

*"La nostra **Visione:** Costruire una rete di partner."*

*"La nostra **Missione:** Garantire la presenza online delle imprese, supportando il lavoro quotidiano delle Web Agency"*

*"I nostri **Valori**: Siamo persone, conosciamo le persone come te, il tuo business e i problemi che ogni giorno affronti, per questo ci concentriamo su valori come il rispetto, la sicurezza, la trasparenza e il supporto."*

CAMPO DI APPLICAZIONE

La presente politica si applica indistintamente a tutti gli organi e i livelli dell'Azienda.
L'attuazione della presente politica è obbligatoria per tutto il personale e deve essere inserita nella regolamentazione degli accordi con qualsiasi soggetto esterno che, a qualsiasi titolo, possa essere coinvolto con il trattamento di informazioni che rientrano nel campo di applicazione del Sistema di Gestione Integrato (SGI).
Tutte le figure professionali facenti parte della struttura, indipendentemente dalle specifiche responsabilità assegnate, sono determinanti per il raggiungimento degli obiettivi di qualità e della sicurezza delle informazioni. L'applicazione dei rispettivi Sistemi di Gestione coinvolge pertanto tutte le funzioni e richiede la partecipazione, l'impegno e l'efficace interazione di tutto il personale dell'organizzazione.

POLITICA SPECIFICA QUALITA'

La Qualità rappresenta per HOST S.p.A. l'obiettivo e lo strumento per:

- il soddisfacimento del Cliente interno ed esterno
- l'eccellenza dei risultati
- la corretta analisi del contesto in cui opera l'azienda
- la corretta valutazione dei rischi e delle opportunità
- il rispetto, la tutela e la promozione della Sicurezza, dell'Ambiente e della Privacy
- la minimizzazione degli sprechi in tempo, costi e altre risorse.

HOST S.p.A. intende perseguire questi obiettivi attraverso:

- organizzazione, tesa a prevenire le non conformità

- servizio, inteso come risposta rapida e professionale alle richieste del Cliente e con equilibrio tra Qualità ed efficienza
- impegno al miglioramento continuo dell'efficacia del Sistema di Gestione della Qualità aziendale.

Gli obiettivi che si pone in ambito qualità sono:
1- DIMINUIRE LE NON CONFORMITA' – Mantenere il livello qualitativo elevato nell'erogazione dei servizi nel rispetto preciso e puntuale delle specifiche sottoscritte contrattualmente con la clientela
2-FORMAZIONE CONTINUA DEL PERSONALE – Avere personale operante in azienda adeguatamente formato rispetto alle attività operative che dovrà svolgere, rispetto alle cogenze legislative (sicurezza, privacy, ecc.) e rispetto ai sistemi di gestione implementati in azienda. Deve essere incoraggiata la piena consapevolezza delle problematiche relative alla sicurezza delle informazioni in tutto il personale (dipendenti e collaboratori) a partire dal momento della selezione e per tutta la durata del rapporto di lavoro
3- LUOGHI DI LAVORO, ATTREZZATURE, MEZZI ED INFRASTRUTTURE MANUTENUTE – Gli asset aziendali devono essere correttamente catalogati, verificate le manutenzioni periodiche ed effettuate a scadenza.
4- LIVELLI DI SERVIZIO RISPETTATI – I Livelli di servizio impostati nei contratti devono essere rispettati e, se possibile, migliorati attraverso l'adozione di best practices aziendali.

POLITICA SPECIFICA SICUREZZA DELLE INFORMAZIONI

Il patrimonio informativo da tutelare è costituito dall'insieme delle informazioni gestite attraverso i servizi forniti e localizzate in tutte le sedi dell'Azienda.
È necessario assicurare:

- la riservatezza delle informazioni: ovvero le informazioni devono essere accessibili solo da chi è autorizzato.
- l'integrità delle informazioni: ovvero proteggere la precisione e la completezza delle informazioni e dei metodi per la loro elaborazione.
- la disponibilità delle informazioni: ovvero che gli utenti autorizzati possano effettivamente accedere alle informazioni e ai beni collegati nel momento in cui lo richiedono.

La mancanza di adeguati livelli di sicurezza può comportare il danneggiamento dell'immagine aziendale, la mancata soddisfazione del cliente, il rischio di incorrere in sanzioni legate alla violazione delle normative vigenti nonché danni di natura economica e finanziaria.
Un adeguato livello di sicurezza è altresì basilare per la condivisione delle informazioni.
L'azienda identifica tutte le esigenze di sicurezza tramite l'analisi dei rischi che incombono sui propri asset aziendali che consente di acquisire idonea consapevolezza sul livello di esposizione a minacce. La valutazione del rischio permette di valutare le potenziali conseguenze e i danni che possono derivare dalla mancata applicazione di misure di sicurezza al sistema informativo e quale sia la realistica probabilità di attuazione delle minacce identificate.
I risultati di questa valutazione determinano le azioni necessarie per gestire i rischi individuati e le misure di sicurezza più idonee.

I Nostri principi della gestione della sicurezza delle informazioni abbracciano i seguenti aspetti:
1- ASSET INVENTORY SEMPRE AGGIORNATO - Garantire un catalogo costantemente aggiornato degli asset aziendali rilevanti ai fini della gestione delle informazioni e per ciascuno deve essere individuato un responsabile. Le informazioni devono essere classificate in base al loro livello di criticità, in modo da essere gestite con livelli di riservatezza ed integrità coerenti ed appropriati.
2- VALUTAZIONE DEI RISCHI DELLE INFORMAZIONI AGGIORNATA – La valutazione dei rischi delle informazioni viene aggiornata almeno una volta all'anno in occasione del riesame della direzione o nel caso si presentino eventi avversi o nel caso vi sia un adeguamento dell'asset inventory.
3- ACCESSO AI SISTEMI SICURO - Per garantire la sicurezza delle informazioni, ogni accesso ai sistemi deve essere sottoposto a una procedura d'identificazione e autenticazione. Le autorizzazioni di accesso alle informazioni devono essere differenziate in base al ruolo ed agli incarichi ricoperti dai singoli individui, in modo che ogni utente possa accedere alle sole informazioni di cui necessita, e devono essere periodicamente sottoposte a revisione.

4- UTILIZZO SICURO DEI BENI AZIENDALI - Devono essere definite delle procedure per l'utilizzo sicuro dei beni aziendali e delle informazioni e dei loro sistemi di gestione.
2-FORMAZIONE CONTINUA DEL PERSONALE – Avere personale operante in azienda adeguatamente formato rispetto alle attività operative che dovrà svolgere, rispetto alle cogenze legislative (sicurezza, privacy, ecc.) e rispetto ai sistemi di gestione implementati in azienda. Deve essere incoraggiata la piena consapevolezza delle problematiche relative alla sicurezza delle informazioni in tutto il personale (dipendenti e collaboratori) a partire dal momento della selezione e per tutta la durata del rapporto di lavoro.
6- GESTIONE TEMPESTIVA DI EVENTI AVVERSI - Per poter gestire in modo tempestivo gli incidenti, tutti devono notificare qualsiasi problema relativo alla sicurezza. Ogni incidente deve essere gestito come indicato nelle procedure.
7- PROTEZIONE FISICA ADEGUATA DELLE SEDI AZIENDALI - È necessario prevenire l'accesso non autorizzato alle sedi e ai singoli locali aziendali dove sono gestite le informazioni e deve essere garantita la sicurezza delle apparecchiature.
8- GESTIONE DELLA COMPLIANCE CONTRATTUALE CON LE TERZE PARTI - Deve essere assicurata la conformità con i requisiti legali e con i principi legati alla sicurezza delle informazioni nei contratti con le terze parti.
9- SIMULAZIONI DEL PIANO DI CONTINUITA' AZIENDALE -Deve essere predisposto un piano di continuità che permetta all'azienda di affrontare efficacemente un evento imprevisto, garantendo il ripristino dei servizi critici in tempi e con modalità che limitino le conseguenze negative sulla missione aziendale.
10- SICUREZZA INFORMATICA BY DESIGN - Gli aspetti di sicurezza devono essere inclusi in tutte le fasi di progettazione, sviluppo, esercizio, manutenzione, assistenza e dismissione dei sistemi e dei servizi informatici.
11- AGGIORNAMENTO LEGISLATIVO CONTINUO - Devono essere garantiti il rispetto delle disposizioni di legge, di statuti, regolamenti o obblighi contrattuali e di ogni requisito inerente la sicurezza delle informazioni, riducendo al minimo il rischio di sanzioni legali o amministrative, di perdite rilevanti o danni alla reputazione.

RESPONSABILITA' DI OSSERVANZA E ATTUAZIONE

L'osservanza e l'attuazione delle policy sono responsabilità di:
1- Tutto il personale che, a qualsiasi titolo, collabora con l'Azienda ed è in qualche modo coinvolto con il trattamento di dati ed informazioni che rientrano nel campo di applicazione del Sistema di Gestione.
Tutto il personale è altresì responsabile della segnalazione di tutte le anomalie e violazioni di cui dovesse venire a conoscenza.

2-Tutti i soggetti esterni che intrattengono rapporti e collaborano con l'Azienda. Devono garantire il rispetto dei requisiti contenuti nella presente policy.

Il Responsabile del Sistema di Gestione, il Responsabile della Sicurezza delle Informazioni e l'Amministrazione del Sistema che, nell'ambito del Sistema di Gestione Integrato e attraverso norme e procedure appropriate, devono:

- condurre l'analisi dei rischi con le opportune metodologie e adottare tutte le misure per la gestione del rischio
- stabilire tutte le norme necessarie alla conduzione sicura di tutte le attività aziendali
- verificare le violazioni alla sicurezza e adottare le contromisure necessarie e controllare l'esposizione dell'azienda alle principali minacce e rischi
- organizzare la formazione e promuovere la consapevolezza del personale per tutto ciò che concerne la sicurezza delle informazioni.
- verificare periodicamente l'efficacia e l'efficienza del Sistema di Gestione.

Chiunque, dipendenti, consulenti e/o collaboratori esterni dell'Azienda, in modo intenzionale o riconducibile a negligenza, disattenda le regole di sicurezza stabilite e in tal modo provochi un danno all'azienda, potrà essere perseguito nelle opportune sedi e nel pieno rispetto dei vincoli di legge e contrattuali.

RIESAME

La Direzione verificherà periodicamente e regolarmente o in concomitanza di cambiamenti significativi l'efficacia e l'efficienza del Sistema di Gestione, in modo da assicurare un supporto adeguato all'introduzione di tutte le migliorie

necessarie e in modo da favorire l'attivazione di un processo continuo, con cui viene mantenuto il controllo e l'adeguamento della policy in risposta ai cambiamenti dell'ambiente aziendale, del business, delle condizioni legali.
Il Responsabile del Sistema di Gestione ha la responsabilità del riesame della politica.
Il riesame dovrà verificare lo stato delle azioni preventive e correttive e l'aderenza alla politica.
Dovrà tenere conto di tutti i cambiamenti che possono influenzare l'approccio della azienda alla gestione della qualità e della sicurezza delle informazioni, includendo i cambiamenti organizzativi, l'ambiente tecnico, la disponibilità di risorse, le condizioni legali, regolamentari o contrattuali e dei risultati dei precedenti riesami.
Il risultato del riesame dovrà includere tutte le decisioni e le azioni relative al miglioramento dell'approccio aziendale alla gestione della qualità e della sicurezza delle informazioni.

IMPEGNO DELLA DIREZIONE

La direzione sostiene attivamente la sicurezza delle informazioni in azienda tramite un chiaro indirizzo, un impegno evidente, degli incarichi espliciti e il riconoscimento delle responsabilità relative alla sicurezza delle informazioni.
L'impegno della direzione si attua tramite una struttura i cui compiti sono:

- garantire che siano identificati tutti gli obiettivi relativi alla sicurezza delle informazioni e che questi incontrino i requisiti aziendali;
- stabilire i ruoli aziendali e le responsabilità per lo sviluppo e il mantenimento del SGI;
- fornire risorse sufficienti alla pianificazione, implementazione, organizzazione, controllo, revisione, gestione e miglioramento continuo del SGI;
- controllare che il SGI sia integrato in tutti i processi aziendali e che procedure e controlli siano sviluppati efficacemente;
- approvare e sostenere tutte le iniziative volte al miglioramento della qualità e sicurezza delle informazioni;
- attivare programmi per la diffusione della consapevolezza e della cultura della qualità e della sicurezza delle informazioni.

Torino, lì 10/05/2022

La Direzione

Marco Mangione