POLITICA AZIENDALE - POLITICA DELLA QUALITA' – POLITICA SICUREZZA DELLE INFORMAZIONI

POLITICA AZIENDALE

Be Team srl, consapevole dell'importanza fondamentale della qualità dei servizi e dei prodotti erogati nonché della protezione, riservatezza, integrità e disponibilità degli asset aziendali, ha implementato ed opera secondo un Sistema di Gestione Integrato (SGI) per la Qualità e la Sicurezza delle Informazioni in conformità agli standard internazionali UNI EN ISO 9001:2015 e UNI CEI EN ISO/IEC 27001:2022.

L'Azienda è convinta che l'adozione e il rigoroso rispetto di tali standard rappresentino non solo un elemento di garanzia e trasparenza verso i mercati, ma anche il motore primario per perseguire la massima soddisfazione di tutte le parti interessate (clienti, dipendenti, collaboratori, fornitori, partner e organi regolatori).

Al fine di perimetrare, mettere in atto e migliorare continuamente il proprio Sistema di Gestione Integrato, Be Team srl analizza e considera sistematicamente le variabili del proprio contesto interno ed esterno, individua e classifica le parti interessate e le relative aspettative, valutando costantemente i rischi strategici ed operativi e le opportunità di sistema.

Nel definire la presente Politica, la Direzione si impegna affinché essa sia pienamente appropriata agli scopi dell'Organizzazione, consenta il miglioramento continuo dell'efficacia ed efficienza dei processi aziendali e garantisca il rigoroso rispetto di tutte le prescrizioni legali, normative e contrattuali applicabili.

CAMPO DI APPLICAZIONE, PERIMETRO (SCOPE) E DICHIARAZIONE DI APPLICABILITA' (SoA)

La presente Politica si applica indistintamente a tutti gli organi, i livelli e le unità organizzative di Be Team srl. L'attuazione delle relative direttive è obbligatoria per tutto il personale dipendente e deve essere recepita e sottoscritta nella regolamentazione degli accordi con qualsiasi soggetto esterno (consulenti, fornitori, partner) coinvolto, a qualsiasi titolo, nel trattamento delle informazioni o nella gestione dei processi aziendali.

Il perimetro specifico del Sistema di Gestione della Sicurezza delle Informazioni (SGSI / ISMS) e della Qualità comprende l'insieme delle sedi, dei processi operativi, delle infrastrutture tecnologiche, delle applicazioni, delle basi dati e delle risorse umane impiegate nella progettazione, sviluppo ed erogazione dei servizi aziendali.

L'individuazione ed attuazione dei controlli di sicurezza delle informazioni di cui all'Allegato A della norma ISO/IEC 27001:2022 è formalizzata all'interno della Dichiarazione di Applicabilità (Statement of Applicability - SoA), documento sottoposto a revisione periodica continua

POLITICA SPECIFICA QUALITA'

Per Be Team srl la qualità rappresenta sia l'obiettivo prioritario sia lo strumento fondamentale per conseguire:

- Soddisfazione del Cliente: Il costante soddisfacimento del Cliente interno ed esterno.
- Eccellenza Operativa: L'eccellenza dei risultati operativi e la continuità prestazionale.
- Analisi del Contesto: La corretta ed aggiornata analisi del contesto competitivo in cui l'Azienda opera.
- Gestione Rischi & Opportunità: La puntuale valutazione dei rischi e la valorizzazione delle opportunità.
- Tutela & Compliance: Il rispetto, la tutela e la promozione della salute e sicurezza sui luoghi di lavoro, dell'ambiente e della protezione dei dati personali (Privacy/GDPR).
- Efficienza delle Risorse: La minimizzazione degli sprechi in termini di tempo, costi ed altre risorse aziendali.

Be Team srl persegue concretamente tali traguardi attraverso:

- Prevenzione Non Conformità: Una struttura organizzativa orientata alla prevenzione attiva delle non conformità e alla gestione tempestiva delle cause radice.
- Orientamento al Servizio: Un servizio caratterizzato da risposte rapide, trasparenti e professionali alle esigenze del Cliente, mantenendo un equilibrio ottimale tra qualità erogata ed efficienza operativa.
- Miglioramento Continuo: Un impegno costante per il miglioramento continuo dell'efficacia del Sistema di Gestione della Qualità.

Indirizzi degli Obiettivi per la Qualità

- Qualità del Servizio: Mantenere elevato ed in costante crescita il livello qualitativo erogato, assicurando il rispetto preciso e puntuale delle specifiche concordate e sottoscritte con il Cliente.
- Formazione del Personale: Incoraggiare ed attuare un piano di formazione continua del personale in relazione alle mansioni operative, alle cogenze legislative ed ai sistemi di gestione adottati.
- Livelli di Servizio (SLA): Rispettare e superare i livelli di servizio (SLA) pattuiti mediante l'adozione di metriche di misurazione oggettive e best practice aziendali.

Gli obiettivi strategici ed operativi dettagliati sono quantificati e riesaminati dalla Direzione almeno una volta all'anno all'interno del Verbale di Riesame della Direzione

POLITICA SPECIFICA PER LA SICUREZZA DELLE INFORMAZIONI

Il patrimonio informativo aziendale e dei Clienti rappresenta un asset strategico primario. Be Team srl garantisce la salvaguardia delle informazioni attraverso il mantenimento dei tre pilastri fondamentali della sicurezza (RID):

- Riservatezza (Confidentiality): Garantire che l'informazione sia accessibile esclusivamente ai soggetti espressamente autorizzati.
- Integrità (Integrity): Salvaguardare l'accuratezza, la completezza ed il valore delle informazioni e dei relativi metodi di elaborazione.
- Disponibilità (Availability): Assicurare che gli utenti autorizzati possano accedere tempestivamente alle informazioni ed ai beni collegati ogni volta che ne facciano richiesta.

La Direzione riconosce che l'inadeguatezza dei livelli di sicurezza può causare gravi danni all'immagine ed alla reputazione aziendale, la perdita di fiducia dei Clienti, l'esposizione a sanzioni amministrative o penali legate alle normative vigenti (es. GDPR, normativa ACN/AgID), nonché perdite di natura economica e finanziaria.

L'Azienda definisce le proprie esigenze di sicurezza mediante una metodologia formale di Valutazione del Rischio (Risk Assessment) condotta sugli asset aziendali. Tale processo consente di identificare minacce e vulnerabilità, stimare la probabilità di accadimento e l'impatto potenziale, guidando l'adozione delle più idonee contromisure di trattamento dei rischi.

Principi Guida per la Gestione della Sicurezza

- Gestione degli Asset IT: Censimento, classificazione ed assegnazione della responsabilità degli asset informatici e materiali.
- Valutazione dei Rischi: Revisione periodica ed aggiornamento continuo della valutazione dei rischi sulle informazioni.
- Controllo Accessi: Adozione del principio del minimo privilegio (Least Privilege) e del controllo accessi logico/fisico sicuro.
- Formazione & Awareness: Programmi continui di addestramento e sensibilizzazione (Security Awareness) per tutto il personale sin dalla fase di selezione e per tutta la durata del rapporto lavorativo.
- Gestione Eventi ed Incidenti: Procedure strutturate per l'identificazione, la segnalazione e la gestione tempestiva degli eventi ed incidenti di sicurezza.
- Protezione Fisica: Misure di protezione fisica, perimetrale ed ambientale idonee a salvaguardare i locali e le infrastrutture aziendali.

- Security by Design: Integrazione della sicurezza fin dalle fasi concettuali e progettuali di nuovi sistemi e servizi (Security & Privacy by Design / Default).
- Aggiornamento Legislativo: Monitoraggio costante dell'evoluzione normativa di settore e della normativa cogente (compresi gli indirizzi AgID e ACN per la Pubblica Amministrazione).

OBIETTIVI DI SICUREZZA DELLE INFORMAZIONI E QUADRO DI MISURABILITA'

Per garantire la conformità alla Clausola 6.2 della norma ISO/IEC 27001:2022, la Direzione definisce un quadro di Obiettivi di Sicurezza delle Informazioni coerenti con la presente Politica, misurabili, monitorati e periodicamente aggiornati. Gli indicatori di prestazione (KPI) includono specificamente:

- KPI Formazione e Consapevolezza: Raggiungimento del 100% del personale dipendente e collaboratore coinvolto nei moduli di formazione e sensibilizzazione sulla sicurezza informatica entro l'anno solare.
- KPI Continuità dei Servizi (Availability): Garantire una disponibilità minima annua pari al 99.5% per i sistemi e servizi informatici critici erogati ai clienti.
- KPI Gestione Incidenti: Presa in carico ed avvio della gestione del 100% degli incidenti di sicurezza segnalati entro 2 ore dalla ricezione ed azzeramento degli incidenti critici non gestiti entro SLA.
- KPI Patching & Vulnerabilità: Applicazione delle patch di sicurezza critiche sui sistemi e server entro 14 giorni dalla pubblicazione del vendor e svolgimento di almeno un Vulnerability Assessment annuo.
- KPI Compliance Legale: Zero sanzioni o contestazioni formali per non conformità alla legislazione sulla protezione dei dati (GDPR) e alle normative di settore.

RUOLI RESPONSABILITA' E CANALE DI SEGNALAZIONE

RESPONSABILITA' GENERALI DEL PERSONALE E DELLE TERZE PARTI

L'osservanza e l'attuazione delle politiche di sicurezza e qualità sono responsabilità di:

- Tutto il Personale: Tutto il personale dipendente e collaboratore che, a qualsiasi titolo, partecipa alle attività aziendali. Ciascun operatore è tenuto a rispettare le procedure operative e a segnalare tempestivamente qualsiasi anomalia, sospetto evento di sicurezza o vulnerabilità rilevata.
- Soggetti Esterni: Tutti i soggetti esterni (fornitori, consulenti, partner) che interagiscono con i sistemi e le informazioni aziendali, i quali devono sottoscrivere ed attenersi ai requisiti espressi nella presente politica e negli accordi contrattuali.

CANALE DI SEGNALAZIONE INCIDENTI

Segnalazione Eventi: Tutte le anomalie, i sospetti incidenti di sicurezza, le perdite di dati o i malfunzionamenti devono essere immediatamente segnalati inviando una comunicazione alla casella di posta dedicata e presidiata:

Email di Contatto: *security@be-team.eu*

CLAUSOLA DISCIPLINARE E SISTEMA SANZIONATORIO

L'osservanza delle prescrizioni contenute nel Sistema di Gestione Integrato costituisce parte integrante degli obblighi contrattuali del personale dipendente e dei collaboratori esterni. La violazione consapevole o negligente delle politiche, delle procedure e delle istruzioni di sicurezza aziendali costituisce inadempimento contrattuale e potrà comportare l'applicazione di sanzioni disciplinari adeguate e proporzionate, secondo quanto previsto dalla legge e dai Contratti Collettivi Nazionali di Lavoro (CCNL) applicabili, oltre all'eventuale risoluzione dei contratti di fornitura per i soggetti esterni e al risarcimento degli eventuali danni arrecati.

RUOLI DI RESPONSABILITA' DEL SISTEMA DI GESTIONE

Il Responsabile del Sistema di Gestione Integrato, il Responsabile della Sicurezza delle Informazioni (CISO) e gli Amministratori di Sistema, nell'ambito delle rispettive competenze, hanno la responsabilità di:

- Analisi Rischi: Condurre ed aggiornare periodicamente l'analisi dei rischi con metodologie formali ed attuare le relative misure di trattamento.
- Procedure Operative: Definire, documentare e mantenere aggiornate le norme e procedure di condotta sicura.

- Gestione Incidenti: Gestire le segnalazioni di violazione della sicurezza, adottare le idonee contromisure ed analizzare l'esposizione aziendale alle minacce.
- Formazione: Pianificare ed organizzare i programmi di formazione e sensibilizzazione per tutto il personale.
- Verifica Efficacia: Verificare e misurare periodicamente l'efficacia ed efficienza complessiva del Sistema di Gestione Integrato

COMUNICAZIONE DIFFUSIONE E DISTRIBUZIONE

La Direzione assicura che la presente Politica sia diffusa, compresa ed applicata a tutti i livelli dell'Organizzazione e resa accessibile alle parti interessate.

Le modalità di comunicazione e diffusione comprendono:

- Comunicazione Interna: Inserimento nel kit d'ingresso (welcome pack) per tutti i neoassunti e pubblicazione nell'area riservata della Intranet aziendale.
- Comunicazione Esterna: Pubblicazione sul sito web aziendale istituzionale per renderla consultabile ai Clienti ed agli stakeholder esterni.

RIESAME DELLA DIREZIONE E MIGLIORAMENTO CONTINUO

La Direzione verifica regolarmente e con frequenza almeno annuale – oppure in concomitanza di significativi cambiamenti organizzativi, tecnologici, di business o normativi – l'adeguatezza, efficacia ed efficienza del Sistema di Gestione Integrato.

Il Responsabile del Sistema di Gestione ha la responsabilità diretta della conduzione delle attività preparatorie per il Riesame della Direzione. Il riesame valuta nello specifico:

- Stato delle Azioni: Lo stato delle azioni correttive, preventive e dei piani di trattamento dei rischi.
- Aderenza agli Obiettivi: L'aderenza effettivo ai principi ed agli obiettivi formulati nella presente Politica.
- Audit & Incidenti: I risultati degli audit interni ed esterni, l'analisi degli incidenti di sicurezza e i feedback dei Clienti.
- Evoluzione del Contesto: I cambiamenti di contesto interno ed esterno, l'adeguatezza delle risorse assegnate e l'evoluzione delle condizioni legali, regolamentari e contrattuali.

Gli esiti del riesame si traducono in decisioni formali volte all'assegnazione delle risorse necessarie ed all'attivazione di azioni per il miglioramento continuo del SGI.

IMPEGNO DELLA DIREZIONE

La Direzione Generale di Be Team srl sostiene e promuove attivamente la cultura della Qualità e della Sicurezza delle Informazioni in Azienda attraverso un chiaro indirizzo strategico, compiti espliciti ed un impegno visibile e continuativo.

Nello specifico, la Direzione si impegna formalmente a:

- Definizione Obiettivi: Garantire l'identificazione, l'approvazione ed il riesame degli obiettivi aziendali per la qualità e la sicurezza.
- Assegnazione Ruoli: Assegnare e formalizzare i ruoli e le responsabilità all'interno dell'organizzazione per il mantenimento del SGI.
- Risorse Adeguate: Fornire risorse umane, tecnologiche e finanziarie adeguate per la pianificazione, attuazione, controllo e miglioramento del SGI.
- Integrazione dei Processi: Promuovere l'integrazione dei requisiti di qualità e sicurezza in tutti i processi di business dell'Azienda.
- Sostegno alle Iniziative: Approvare e sostenere prioritariamente tutte le iniziative volte all'accrescimento della sicurezza informatica e della qualità dei servizi.

Rivoli, li 03/11/2026 La Direzione