POL Politica di sicurezza delle informazioni

Nome della società	Logic Solution
Data di entrata in vigore	25/05/2024

Storia della versione

Versione	Data	Descrizione	Autore	Approvato da
1	25/05/2024	-- N / D --		

Scopo

Lo scopo della presente politica è dichiarare e comunicare l'impegno del Top Management verso la protezione degli asset informativi dell'organizzazione. Questo documento definisce il quadro di riferimento per istituire, attuare, mantenere e migliorare continuamente il Sistema di Gestione della Sicurezza delle Informazioni (SGSI), al fine di proteggere la riservatezza, l'integrità e la disponibilità delle informazioni e di supportare gli obiettivi strategici aziendali.

Indice

- Campo di Applicazione
- Riferimenti Normativi
- Termini e Definizioni
- Ruoli e Responsabilità
- Obiettivi di sicurezza delle informazioni
- Principi fondamentali di sicurezza delle informazioni
- Gestione e Revisione della Politica
- Responsabilità Condivisa
- Uso Accettabile delle Risorse
- Protezione degli Asset
- Segnalazione degli Eventi di Sicurezza
- Archiviazione e Aggiornamenti
- Documenti di Riferimento

Campo di Applicazione

La presente politica stabilisce il quadro di riferimento per la gestione della sicurezza delle informazioni in Logic Solution. Il suo scopo è proteggere il patrimonio informativo aziendale da minacce interne ed esterne, intenzionali o accidentali, garantendo la continuità operativa e la conformità ai requisiti legali e normativi. Questo documento si applica a tutte le informazioni gestite dall'azienda, indipendentemente dal formato, e a tutto il personale, ai collaboratori e alle terze parti che hanno accesso alle risorse informative di Logic Solution.

Riferimenti Normativi

- **ISO/IEC 27001:2022**: Sicurezza delle informazioni, sicurezza informatica e protezione della privacy — Sistemi di gestione della sicurezza delle informazioni — Requisiti.
- **Regolamento (UE) 2016/679 (GDPR)**: Relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.
- **Decreto Legislativo 81/2008**: Testo unico sulla salute e sicurezza sul lavoro

Termini e Definizioni

- **Riservatezza**: La proprietà che le informazioni non siano rese disponibili o divulgate a individui, entità o processi non autorizzati.
- **Integrità**: La proprietà di salvaguardare l'accuratezza e la completezza degli asset.
- **Disponibilità**: La proprietà di essere accessibile e utilizzabile su richiesta da un'entità autorizzata.
- **Sistema di Gestione della Sicurezza delle Informazioni (SGSI)**: Un insieme di policy e procedure per gestire sistematicamente i dati sensibili di un'organizzazione. L'obiettivo di un SGSI è minimizzare il rischio e garantire la continuità operativa proteggendo proattivamente le informazioni.

Ruoli e Responsabilità

- **Direzione Generale (DIR)**: Definisce e approva la politica per la sicurezza delle informazioni, supervisiona l'attuazione del SGSI e assicura l'allocazione delle risorse necessarie per la sua efficacia.
- **Responsabile SGSI**: Supporta la documentazione e il controllo del SGSI, pianifica gli audit interni sulla sicurezza delle informazioni e monitora la gestione delle non conformità e delle azioni correttive.
- **Responsabile IT**: Assicura la gestione tecnica degli accessi agli asset informatici e la messa in sicurezza dell'infrastruttura IT in conformità con le policy aziendali.
- **Tecnico IT**: Applica le misure tecniche e operative previste dal SGSI, fornisce supporto nella gestione quotidiana della sicurezza e segnala eventi o vulnerabilità.

Obiettivi di sicurezza delle informazioni

Logic Solution si impegna a proteggere il proprio patrimonio informativo da tutte le minacce, interne o esterne, intenzionali o accidentali, al fine di assicurare la continuità operativa, minimizzare i rischi e massimizzare le opportunità di business. La Direzione Generale (DIR) definisce e approva gli obiettivi strategici di sicurezza, che si fondano sulla salvaguardia della riservatezza, integrità e disponibilità delle informazioni.

Per raggiungere tali scopi, Logic Solution istituisce e mantiene attivo un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) conforme ai requisiti dello standard internazionale ISO/IEC 27001. Gli obiettivi specifici del SGSI sono definiti in coerenza con il contesto aziendale, gli obblighi legali e contrattuali e gli esiti della valutazione dei rischi, come formalizzato nella "PRO Procedura di gestione dei rischi" e gestiti tramite la "PRO Obiettivi e pianificazione per il loro raggiungimento".

Il Responsabile SGSI ha la responsabilità di tradurre gli indirizzi strategici in obiettivi misurabili e di monitorarne il raggiungimento, garantendo un allineamento costante tra le strategie di business e la tutela delle informazioni.

Principi fondamentali di sicurezza delle informazioni

Gestione e Revisione della Politica

La presente politica è approvata dalla Direzione Generale (DIR) e costituisce il documento di vertice del SGSI.

Il Responsabile SGSI deve:

- Rivedere questa politica a intervalli pianificati, e comunque ogni qualvolta si verifichino cambiamenti significativi, in accordo con la "PRO Procedura di gestione del cambiamento" e gli esiti del "PRO Gestione riesame della direzione".
- Assicurare che la politica sia comunicata a tutto il personale e alle parti interessate rilevanti, rendendola disponibile secondo quanto previsto dalla "PRO Procedura di gestione delle informazioni documentate".

Responsabilità Condivisa

La sicurezza delle informazioni è una responsabilità condivisa che coinvolge tutto il personale di Logic Solution. Ogni dipendente e collaboratore è tenuto a proteggere le informazioni e le risorse aziendali con cui entra in contatto durante lo svolgimento delle proprie mansioni. Le responsabilità specifiche sono dettagliate nella "POL Politica dei ruoli e delle responsabilità in materia di sicurezza delle informazioni".

Uso Accettabile delle Risorse

L'utilizzo di tutte le informazioni, degli asset IT e delle risorse associate è consentito esclusivamente per scopi aziendali legittimi e autorizzati. L'accesso alle informazioni si basa sui principi di minimo privilegio e necessità operativa, come disciplinato dalla "PRO Procedura di gestione e controllo degli accessi logici".

Il Responsabile IT deve assicurare che gli accessi siano formalmente autorizzati e tracciati. A supporto di questo principio, viene mantenuto il "Registro degli utenti autorizzati all'uso delle informazioni". Tutto il personale è tenuto a conformarsi alle norme di comportamento definite nel "Codice di condotta" aziendale.

Protezione degli Asset

Politica della Scrivania e dello Schermo Puliti (Clear Desk and Clear Screen): Tutto il personale deve adottare le seguenti misure per ridurre il rischio di accessi non autorizzati, perdita o danneggiamento delle informazioni:

- Le postazioni di lavoro devono essere lasciate libere da documenti sensibili e supporti di memorizzazione rimovibili quando incustodite.
- I dispositivi informatici devono essere bloccati quando l'utente si allontana. Tutte le postazioni di lavoro devono essere configurate per attivare il blocco automatico dello schermo dopo un periodo massimo di 15 minuti di inattività e richiedere l'inserimento della password per riprendere la sessione.
- I documenti cartacei e i supporti di memorizzazione devono essere custoditi in modo sicuro, in linea con quanto stabilito nella "POL Politica di classificazione ed etichettatura delle informazioni" e nella "POL Politica di conservazione e cancellazione delle informazioni".

Sicurezza degli Asset Fuori Sede: Gli asset aziendali utilizzati al di fuori delle sedi di Logic Solution, inclusi quelli impiegati per il lavoro da remoto, devono essere protetti con lo stesso livello di diligenza applicato all'interno degli uffici. Il personale che opera in modalità remota deve:

- Connettersi alla rete aziendale esclusivamente tramite il client VPN approvato (OpenVPN).
- Assicurarsi che i controlli di sicurezza forniti dall'azienda, come antivirus e firewall, siano sempre attivi e non vengano disattivati o modificati.
- Adottare le regole di scrivania e schermo puliti anche nel proprio ambiente di lavoro remoto. Ulteriori disposizioni sono contenute nella "POL Politica di sicurezza operativa".

Segnalazione degli Eventi di Sicurezza

Tutto il personale ha l'obbligo di segnalare tempestivamente qualsiasi evento, anomalia o debolezza di sicurezza osservata o sospetta. Le segnalazioni devono essere effettuate attraverso i canali definiti nella "PRO Procedura di gestione degli incidenti di sicurezza delle informazioni", rivolgendosi al Tecnico IT o al Responsabile IT a seconda della gravità.

Archiviazione e Aggiornamenti

La presente politica è soggetta a revisione periodica, almeno annuale, e ogni qualvolta si verifichino cambiamenti organizzativi, tecnologici o normativi rilevanti. Il Responsabile SGSI è incaricato della revisione, mentre l'approvazione delle modifiche spetta alla Direzione Generale (DIR). La gestione e l'archiviazione del documento seguono le procedure interne per le informazioni documentate.

Documenti di Riferimento

- PRO Procedura di gestione dei rischi
- PRO Obiettivi e pianificazione per il loro raggiungimento
- PRO Procedura di gestione del cambiamento
- PRO Gestione riesame della direzione

- PRO Procedura di gestione delle informazioni documentate
- POL Politica dei ruoli e delle responsabilità in materia di sicurezza delle informazioni
- PRO Procedura di gestione e controllo degli accessi logici
- Registro degli utenti autorizzati all'uso delle informazioni
- Codice di condotta
- POL Politica di classificazione ed etichettatura delle informazioni
- POL Politica di conservazione e cancellazione delle informazioni
- POL Politica di sicurezza operativa
- PRO Procedura di gestione degli incidenti di sicurezza delle informazioni