Sintia

Pubblico

POL Politica di sicurezza delle informazioni

Nome della società	Sintia
Data di entrata in vigore	08/06/2024

Storia della versione

Versione	Data	Descrizione	Autore	Approvato da
1	08/06/2024	-- N/D --	Alessandra Arcuri	Alessio Mosto

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

La presente politica definisce i principi e gli obiettivi strategici per la gestione della sicurezza delle informazioni in Sintia Lab. Il suo scopo è proteggere gli asset informativi dell'azienda e dei suoi clienti, garantendo la continuità operativa, la conformità normativa e la fiducia delle parti interessate. Questo documento si applica a tutto il personale, ai processi, ai dati e alle tecnologie che rientrano nel perimetro del Sistema di Gestione Integrato (SGI).

Riferimenti normativi

- ISO 27001
- ISO 27017
- ISO 27018

Termini e definizioni

- **Riservatezza** : Proprietà per cui le informazioni non vengono rese disponibili o divulgate a persone, entità o processi non autorizzati.
- **Integrità** : Proprietà di salvaguardare l'accuratezza e la completezza degli asset.
- **Disponibilità** : Proprietà di essere accessibile e utilizzabile su richiesta da un'entità autorizzata.
- **Informazioni Personali Identificabili (PII)** : Qualsiasi informazione che può essere utilizzata per identificare una persona specifica.
- **Cliente di servizi cloud (Cloud Service Customer)** : L'organizzazione o la persona che utilizza i servizi cloud.

Ruoli e responsabilità

- **Amministratore Unico** : Ha la responsabilità ultima della sicurezza delle informazioni, approva la relativa politica e garantisce la disponibilità delle risorse necessarie per l'attuazione e il mantenimento del Sistema Integrato.
- **RSGI (Responsabile del Sistema di Gestione Integrato)** : È responsabile della supervisione, implementazione e mantenimento del Sistema di Gestione Integrato, inclusa la sicurezza delle informazioni, e riporta direttamente all'Amministratore Unico.
- **Enterprise IT** : È responsabile della gestione operativa della sicurezza dei sistemi informativi, della configurazione dei controlli di sicurezza, della gestione degli accessi e della presa in carico degli eventi di sicurezza.

Obiettivi di sicurezza delle informazioni

Sintia Lab si impegna a proteggere i propri asset informativi e quelli dei suoi clienti per garantire la continuità del business, minimizzare i rischi e massimizzare le opportunità di crescita. L'Amministratore Unico ha la responsabilità ultima della sicurezza delle informazioni e approva la presente politica, assicurando la disponibilità delle risorse necessarie al suo mantenimento.

Gli obiettivi strategici del Sistema di Gestione Integrato (SGI) sono:

- **Riservatezza** : Assicurare che le informazioni siano accessibili solo al personale autorizzato, proteggendo i dati sensibili, la proprietà intellettuale e le informazioni personali (PII) da accessi non autorizzati.
- **Integrità** : Salvaguardare l'accuratezza e la completezza delle informazioni e dei metodi di elaborazione, prevenendo modifiche, cancellazioni o danneggiamenti non autorizzati.
- **Disponibilità** : Garantire che il personale autorizzato abbia accesso alle informazioni e agli asset associati quando necessario, assicurando la resilienza dei processi di business.

Questi obiettivi sono perseguiti in conformità ai requisiti legali, normativi e contrattuali applicabili e sono riesaminati periodicamente per assicurarne la continua adeguatezza. La definizione, la pianificazione e il monitoraggio degli obiettivi operativi sono gestiti secondo quanto descritto nella procedura "PRO Obiettivi e pianificazione per il loro raggiungimento".

Principi fondamentali di sicurezza delle informazioni

Gestione e Revisione della Politica

L'approccio di Sintia Lab alla sicurezza delle informazioni si fonda sui seguenti principi:

- **Approccio basato sul rischio** : Le decisioni in materia di sicurezza delle informazioni sono guidate da un processo strutturato di valutazione e trattamento dei rischi, come definito nella "PRO Procedura di gestione dei rischi".
- **Responsabilità condivisa** : La sicurezza delle informazioni è una responsabilità di tutto il personale, sotto la guida dell'Amministratore Unico. I ruoli e le responsabilità specifiche sono formalizzati nella "POL Politica dei ruoli e delle responsabilità in materia di sicurezza delle informazioni".
- **Conformità normativa e contrattuale** : L'organizzazione si impegna a rispettare tutte le leggi applicabili, inclusa la normativa sulla protezione dei dati personali (PII), e gli obblighi contrattuali sottoscritti con clienti e fornitori.
- **Miglioramento continuo** : Il SGSI è soggetto a un processo di miglioramento continuo per aumentarne l'efficacia e l'adeguatezza nel tempo.

L'Amministratore Unico deve approvare la presente politica e i documenti ad essa correlati. La politica è comunicata a tutto il personale e alle parti interessate rilevanti e deve essere riesaminata con cadenza almeno annuale, o a seguito di cambiamenti significativi, come disciplinato nella "PRO Procedura di gestione del cambiamento".

Uso delle Risorse Aziendali

- **Uso Accettabile** : Tutto il personale deve utilizzare le informazioni e gli asset aziendali, inclusi i sistemi IT e le connessioni di rete, esclusivamente per scopi lavorativi e in conformità con le regole definite nel "Codice di condotta" e nella "POL Politica di sicurezza operativa". L'assegnazione e la gestione degli asset sono formalizzate tramite il "MOD Modulo di assegnazione dei beni".
- **Scrivania Pulita e Schermo Pulito** : Il personale deve assicurare che documenti cartacei e supporti di memorizzazione rimovibili contenenti informazioni sensibili non siano lasciati incustoditi. Le postazioni di lavoro devono essere bloccate quando non presidiate e la sessione di lavoro deve essere chiusa al termine dell'attività. L'Enterprise IT deve garantire che su tutte le postazioni sia configurato un blocco schermo automatico dopo un breve periodo di inattività.
- **Sicurezza degli Asset Fuori Sede e Lavoro da Remoto** : Gli asset aziendali utilizzati al di fuori delle sedi aziendali, inclusi quelli per il lavoro da remoto, devono essere protetti con lo stesso livello di sicurezza richiesto in sede. Il personale è direttamente responsabile della custodia e della protezione degli asset ricevuti in dotazione. Le modalità di lavoro da remoto e l'uso di dispositivi mobili sono disciplinate nel rispetto della "POL Politica di sicurezza operativa".

Sicurezza nell'Utilizzo dei Servizi Cloud

Sintia Lab, in qualità di cliente di servizi cloud (cloud service customer), adotta un approccio basato sul rischio per la selezione e l'utilizzo di tali servizi.

- L'Amministratore Unico deve garantire che gli accordi contrattuali con i fornitori di servizi cloud definiscano chiaramente il modello di responsabilità condivisa per la sicurezza e la protezione dei dati.
- La valutazione dei fornitori cloud deve considerare i rischi associati alla multi-tenancy, all'accesso ai dati da parte del fornitore e alla localizzazione geografica dei dati.
- L'Enterprise IT deve gestire gli accessi privilegiati ai servizi cloud secondo il principio del minimo privilegio e assicurare la corretta configurazione dei controlli di sicurezza disponibili.
- Ulteriori requisiti sono dettagliati nella "POL Politica di sicurezza del cloud".

Protezione delle Informazioni Personali (PII)

Sintia Lab si impegna a garantire la conformità con la legislazione applicabile in materia di protezione delle Informazioni Personali Identificabili (PII) e con i termini contrattuali concordati. Questo impegno si estende a tutti i dati personali trattati, inclusi quelli gestiti tramite servizi cloud di terze parti. L'Amministratore Unico garantisce che l'utilizzo di tali servizi avvenga secondo criteri di sicurezza e protezione dei dati definiti. Le responsabilità e le modalità di trattamento sono ulteriormente specificate nella "POL Politica di protezione delle PII".

Segnalazione degli Eventi di Sicurezza

Tutto il personale ha l'obbligo di segnalare tempestivamente qualsiasi evento di sicurezza delle informazioni osservato o sospetto, nonché ogni debolezza dei sistemi. Le segnalazioni devono essere effettuate attraverso i canali appropriati definiti nella "PRO Procedura di gestione degli incidenti di sicurezza delle informazioni". L'Enterprise IT è responsabile della presa in carico e della gestione iniziale degli eventi segnalati.

Archiviazione e aggiornamenti

Questo documento è archiviato nel sistema di gestione documentale aziendale. Sarà riesaminato con cadenza almeno annuale e aggiornato ogni qualvolta si verifichino cambiamenti significativi nei processi, nell'organizzazione o nei requisiti di sicurezza applicabili, sotto la supervisione dell'Amministratore Unico.

Documenti di riferimento

- PRO Obiettivi e pianificazione per il loro raggiungimento
- PRO Procedura di gestione dei rischi
- POL Politica dei ruoli e delle responsabilità in materia di sicurezza delle informazioni
- PRO Procedura di gestione del cambiamento
- Codice di condotta
- POL Politica di sicurezza operativa
- MOD Modulo di assegnazione dei beni
- POL Politica di sicurezza del cloud
- POL Politica di protezione delle PII
- PRO Procedura di gestione degli incidenti di sicurezza delle informazioni