POL Politica di sicurezza delle informazioni

Nome della società	Aptus
Data di entrata in vigore	10/07/2024

Storia della versione

Versione	Data	Descrizione	Autore	Approvato da
1	10/07/2024	-- N / D --	Enrico Lucia	Lorenzo De mattei

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 stabilisce i principi e le direttive fondamentali per la gestione della sicurezza delle informazioni in Aptus. Il suo scopo è proteggere gli asset informativi dell'organizzazione per assicurare la continuità operativa, minimizzare i rischi e garantire la conformità ai requisiti legali e contrattuali. Le disposizioni di questo documento si applicano a tutto il personale, ai processi, ai dati e alle tecnologie che rientrano nel perimetro del Sistema di Gestione della Sicurezza delle Informazioni (SGSI).

Riferimenti Normativi

- **ISO/IEC 27001:2022**: Sistemi di gestione per la sicurezza delle informazioni — Requisiti.
- **Regolamento (UE) 2016/679 (GDPR)**: Regolamento Generale sulla Protezione dei Dati.

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.

Ruoli e Responsabilità

- **Top Management**: Assume la responsabilità ultima per l'efficacia del Sistema di Gestione della Sicurezza delle Informazioni, approvando la relativa politica e assicurando la disponibilità delle risorse necessarie al suo mantenimento e miglioramento.
- **ISMS Manager**: Assicura la definizione, l'implementazione, il mantenimento e il miglioramento continuo del Sistema di Gestione della Sicurezza delle Informazioni in conformità con la presente politica e gli standard di riferimento.
- **HR Specialist**: Gestisce gli aspetti relativi alla sicurezza delle informazioni nel ciclo di vita del personale, assicurando che i dipendenti prendano visione e accettino le politiche di sicurezza aziendali al momento dell'assunzione e in occasione di aggiornamenti.
- **VP of Compliance & Legal**: Supervisiona l'identificazione e il monitoraggio dei requisiti legali, normativi e contrattuali applicabili alla sicurezza delle informazioni, garantendone l'integrazione all'interno del SGSI.
- **Compliance Specialist**: Supporta il monitoraggio della conformità aziendale ai requisiti di sicurezza, alle policy interne e agli standard di riferimento, collaborando alla gestione dei rischi e alla conduzione di audit.

Obiettivi di sicurezza delle informazioni

Aptus si impegna a proteggere i propri asset informativi per garantire la continuità del business, minimizzare i danni e massimizzare il ritorno sugli investimenti e le opportunità di business. L'obiettivo primario del Sistema di Gestione della Sicurezza delle Informazioni (SGSI) è quello di assicurare la riservatezza, l'integrità e la disponibilità delle informazioni

trattate. Il Top Management definisce e riesamina periodicamente gli obiettivi di sicurezza delle informazioni, assicurando che siano misurabili, coerenti con il contesto aziendale e allineati ai requisiti legali, normativi e contrattuali. La definizione e la pianificazione di tali obiettivi sono formalizzate nel documento "PRO Obiettivi e pianificazione per il loro raggiungimento".

Gli obiettivi strategici di Aptus includono:

- Garantire la conformità con le leggi e i regolamenti applicabili, inclusi quelli sulla protezione dei dati personali.
- Proteggere le informazioni dei clienti e i segreti commerciali da accessi, modifiche o divulgazioni non autorizzate.
- Assicurare che i servizi erogati ai clienti siano resilienti e disponibili secondo i termini contrattuali.
- Promuovere una cultura della sicurezza in cui tutto il personale sia consapevole delle proprie responsabilità.
- Migliorare continuamente l'efficacia del SGSI attraverso il monitoraggio delle prestazioni e l'analisi dei rischi.

La responsabilità della supervisione e del raggiungimento di questi obiettivi è del Top Management, con il supporto del ISMS Manager.

Principi fondamentali di sicurezza delle informazioni

Governo della Sicurezza

Il Top Management approva la presente politica e tutte le politiche specifiche per argomento, dimostrando il proprio impegno verso la sicurezza delle informazioni. Il ISMS Manager ha la responsabilità di assicurare che tutta la documentazione del SGSI, inclusa la presente politica, sia pubblicata, comunicata a tutto il personale e alle parti interessate rilevanti, e mantenuta aggiornata.

La revisione della documentazione del SGSI è condotta a intervalli pianificati e ogni qualvolta si verifichino cambiamenti significativi, in accordo con le procedure "PRO Gestione riesame della direzione" e "PRO Procedura di gestione del cambiamento". La gestione di tutta la documentazione è descritta nella "PRO Procedura di gestione delle informazioni documentate".

L'HR Specialist assicura che tutto il personale prenda visione e accetti le politiche di sicurezza delle informazioni in fase di assunzione e in occasione di aggiornamenti significativi.

Approccio Basato sul Rischio

Aptus adotta un approccio alla sicurezza delle informazioni basato sulla gestione del rischio. Tutte le misure di controllo sono implementate in seguito a un'attenta valutazione dei rischi per gli asset informativi. L'ISMS Manager supervisiona questo processo, che è formalizzato nella "PRO Procedura di gestione dei rischi", per garantire che i rischi siano identificati, analizzati e trattati in modo adeguato.

Ruoli e Responsabilità

La sicurezza delle informazioni è una responsabilità condivisa da tutto il personale di Aptus. Il Top Management detiene la responsabilità ultima per l'efficacia del SGSI. Ruoli e responsabilità specifici in materia di sicurezza sono definiti e assegnati formalmente nel documento "POL Politica dei ruoli e delle responsabilità in materia di sicurezza delle informazioni" e integrati nei mansionari aziendali.

Uso Accettabile delle Risorse

Tutto il personale è tenuto a utilizzare le informazioni, i sistemi informatici, le reti e le altre risorse associate esclusivamente per scopi aziendali autorizzati e in conformità con le normative vigenti e le direttive interne. È severamente vietato l'uso delle risorse aziendali per attività illecite o che possano compromettere la sicurezza dell'organizzazione. Le regole dettagliate per l'uso accettabile sono definite nella "POL Politica di sicurezza operativa" e nel "Codice di condotta".

Protezione degli Asset Informativi

- **Classificazione delle Informazioni**: Tutti gli asset informativi devono essere classificati in base alla loro criticità, valore e sensibilità, come stabilito nella "POL Politica di classificazione ed etichettatura delle informazioni". Le misure di protezione applicate devono essere proporzionate al livello di classificazione.
- **Sicurezza degli Ambienti di Lavoro (Clear Desk e Clear Screen)**: Il personale deve garantire che le informazioni sensibili, sia in formato cartaceo che digitale, siano protette da accessi non autorizzati. Ciò include l'obbligo di bloccare la propria postazione di lavoro quando incustodita (schermo pulito) e di custodire in modo sicuro documenti e supporti di memorizzazione rimovibili al termine della giornata lavorativa (scrivania pulita).
- **Sicurezza degli Asset Fuori Sede**: Gli asset aziendali utilizzati al di fuori delle sedi di Aptus, inclusi i dispositivi impiegati per il lavoro agile, devono essere protetti con misure adeguate contro il furto, la perdita, il danneggiamento e l'accesso non autorizzato. Ogni dipendente è responsabile della protezione fisica e logica dei dispositivi affidatigli e della riservatezza delle informazioni trattate in modalità remota, come specificato nell'accordo individuale di lavoro agile e nella "POL Politica di sicurezza operativa".

Segnalazione degli Eventi di Sicurezza

Tutto il personale ha l'obbligo di segnalare tempestivamente qualsiasi evento, debolezza o incidente di sicurezza delle informazioni, osservato o sospetto. I canali e le modalità di segnalazione sono definiti nella "PRO Procedura di gestione degli incidenti di sicurezza delle informazioni". L'ISMS Manager garantisce che il processo di segnalazione sia noto a tutto il personale.

Conformità

Aptus si impegna a rispettare tutti i requisiti legali, normativi e contrattuali applicabili alla sicurezza delle informazioni. Il VP of Compliance & Legal e il Compliance Specialist sono responsabili dell'identificazione e del monitoraggio di tali requisiti, assicurando che siano integrati nel SGSI.

Archiviazione e Aggiornamenti

La presente politica è gestita come informazione documentata del SGSI. Viene riesaminata con cadenza almeno annuale, e ogni qualvolta si verifichino cambiamenti significativi nel contesto interno o esterno, dal ISMS Manager e approvata dal Top Management per garantirne la continua idoneità, adeguatezza ed efficacia.

Documenti di Riferimento

- PRO Obiettivi e pianificazione per il loro raggiungimento
- PRO Gestione riesame della direzione
- PRO Procedura di gestione del cambiamento
- PRO Procedura di gestione delle informazioni documentate
- PRO Procedura di gestione dei rischi
- POL Politica dei ruoli e delle responsabilità in materia di sicurezza delle informazioni
- POL Politica di sicurezza operativa
- Codice di condotta
- POL Politica di classificazione ed etichettatura delle informazioni
- PRO Procedura di gestione degli incidenti di sicurezza delle informazioni