POL Politica di sicurezza operativa

Nome della società	Partech
Data di entrata in vigore	22/04/2025

Storia della versione

Versione	Data	Descrizione	Autore	Approvato da
1	22/04/2025	-- N / D --	Fabio Damiani	Giuseppe Favilli

Scopo

Lo scopo di questa politica è garantire il funzionamento corretto, sicuro e resiliente di tutti i sistemi, le reti e le strutture di elaborazione delle informazioni dell'organizzazione. Infatti, la presente politica definisce i controlli e le procedure necessarie per proteggere la riservatezza, l'integrità e la disponibilità delle informazioni durante le operazioni quotidiane, riducendo al minimo i rischi di interruzione del servizio, perdita di dati e incidenti di sicurezza.

Indice

Campo di Applicazione

La presente politica definisce le regole e le procedure per garantire la sicurezza operativa delle informazioni, dei sistemi e degli asset di Partech. Lo scopo è proteggere le risorse informative da minacce interne ed esterne, assicurando la conformità ai requisiti legali, normativi e contrattuali. Le disposizioni di questo documento si applicano a tutto il personale e alle terze parti che hanno accesso agli asset informativi aziendali.

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

- **Dati Personali (PII - Personally Identifiable Information)**: Qualsiasi informazione che, da sola o in combinazione con altre, può essere utilizzata per identificare, contattare o localizzare un singolo individuo.

Ruoli e Responsabilità

- **CEO / Direzione Generale**: Approva le strategie di sicurezza, assicura la disponibilità delle risorse necessarie per la gestione del rischio e supervisiona la conformità complessiva alle policy aziendali.
- **Executive - Acquisti**: Assicura che i fornitori rispettino le politiche di sicurezza aziendali e che i contratti includano clausole adeguate per la protezione dei dati e la sicurezza delle informazioni.
- **Executive - Cybersecurity e Privacy**: Definisce la strategia di sicurezza, gestisce il rischio informatico, supervisiona la risposta agli incidenti e garantisce la conformità normativa in materia di cybersecurity e privacy.
- **Responsabile IT / Infrastructure & Operations**: Guida la gestione dell'infrastruttura tecnologica, definisce gli standard tecnici e garantisce l'affidabilità, le prestazioni e la sicurezza dei servizi IT interni, supervisionando l'applicazione delle procedure operative descritte in questo documento.
- **Responsabile Privacy & GDPR**: Supervisiona l'applicazione della normativa sulla protezione dei dati personali, funge da punto di contatto per le autorità di controllo e gli interessati e coordina la gestione dei trattamenti dei dati.
- **Tecnico - Sistemista**: Esegue le attività operative per garantire il corretto funzionamento, la sicurezza e la protezione dei sistemi informatici e dei dati, in conformità con le procedure definite.

Backup

Gestione e Pianificazione dei Backup

Il Responsabile IT / Infrastructure & Operations ha la responsabilità di definire, documentare e mantenere una strategia di backup per tutte le informazioni, i software e i sistemi critici per l'operatività aziendale. La frequenza e la tipologia dei backup devono

essere stabilite in base alla criticità dei dati, ai requisiti di business e agli obblighi contrattuali e legali, come definito nella "POL Politica di classificazione ed etichettatura delle informazioni". Le attività operative di esecuzione, monitoraggio e verifica dei job di backup sono assegnate al Tecnico - Sistemista, che opera sotto la supervisione del Responsabile IT / Infrastructure & Operations.

Protezione e Conservazione dei Backup

Tutte le copie di backup devono essere protette da accessi non autorizzati, modifiche, distruzione e divulgazione. Il Responsabile IT / Infrastructure & Operations deve garantire l'implementazione di misure di sicurezza adeguate, tra cui:

- **Controllo degli Accessi**: L'accesso ai dati di backup e ai sistemi di gestione dei backup deve essere limitato al solo personale autorizzato, secondo il principio del minimo privilegio definito nella "PRO Procedura di gestione e controllo degli accessi logici".
- **Crittografia**: I dati di backup devono essere protetti tramite crittografia sia durante il transito sia a riposo (at-rest), in conformità con la "PRO Procedura di crittografia e gestione delle chiavi crittografiche".
- **Conservazione**: I backup devono essere conservati per il periodo di tempo definito nella "POL Politica di conservazione e cancellazione delle informazioni", assicurando che siano eliminati in modo sicuro al termine del loro ciclo di vita.

Ridondanza e Test di Ripristino

Per garantire la disponibilità e la resilienza, il Responsabile IT / Infrastructure & Operations deve assicurare che le copie di backup siano archiviate in modo ridondante. Ciò include la conservazione di almeno una copia in una posizione geograficamente separata (off-site). Devono essere eseguiti test di ripristino a intervalli pianificati per verificare l'integrità, l'affidabilità e l'efficacia delle procedure di backup. Il Responsabile IT / Infrastructure & Operations è responsabile della pianificazione e della supervisione di tali test, nonché della documentazione dei risultati. Le procedure operative per il ripristino sono dettagliate nella "PRO Procedura di continuità operativa e di ripristino di emergenza".

Protezione dei dati personali

Conformità Normativa

Partech si impegna a identificare e soddisfare tutti i requisiti derivanti da leggi, regolamenti e contratti applicabili in materia di privacy e protezione dei dati personali (PII), con particolare riferimento al GDPR (Regolamento UE 2016/679). La CEO / Direzione Generale approva le strategie e fornisce le risorse necessarie per garantire la conformità.

Il Responsabile Privacy & GDPR ha la responsabilità di supervisionare l'applicazione della normativa, fungendo da punto di contatto con le autorità di controllo e gli interessati.

Gestione dei Trattamenti e Valutazione dei Rischi

Il Responsabile Privacy & GDPR deve mantenere e aggiornare il registro delle attività di trattamento, come formalizzato nel documento "MOD Registro dei trattamenti del titolare".

Per ogni nuovo trattamento di dati personali o in caso di modifiche significative a trattamenti esistenti che possano presentare un rischio elevato per i diritti e le libertà degli interessati, l'Executive - Cybersecurity e Privacy deve condurre una Valutazione d'Impatto

sulla Protezione dei Dati (DPIA). Tutto il personale che tratta dati personali è tenuto a rispettare i principi di liceità, correttezza, trasparenza, minimizzazione dei dati e limitazione della finalità, come indicato nelle informative fornite agli interessati e nella "PRO Procedura di gestione delle risorse umane".

Gestione dei log

Produzione e Conservazione dei Log

Il Responsabile IT / Infrastructure & Operations deve garantire che tutti i sistemi informativi, le reti e le applicazioni producano registrazioni (log) per tracciare eventi significativi. Tali eventi includono, ma non si limitano a, accessi (riusciti e falliti), attività degli utenti con privilegi elevati, errori di sistema, modifiche alle configurazioni di sicurezza e attività di gestione dei dati.

I log devono essere protetti da manomissioni, accessi non autorizzati e distruzione impropria. Le politiche di conservazione dei log sono definite nella "POL Politica di conservazione e cancellazione delle informazioni". L'accesso ai log è regolamentato dalla "PRO Procedura di gestione e controllo degli accessi logici".

Sincronizzazione degli Orologi

Tutti gli orologi dei sistemi di elaborazione delle informazioni devono essere sincronizzati con una fonte di tempo di riferimento approvata dal Responsabile IT / Infrastructure & Operations. Questa misura è obbligatoria per garantire la coerenza cronologica degli eventi registrati nei log e facilitare le attività di correlazione e analisi.

Monitoraggio e Analisi

L'Executive - Cybersecurity e Privacy, in collaborazione con il Responsabile IT / Infrastructure & Operations, ha la responsabilità di definire e implementare attività di monitoraggio continuo su reti, sistemi e applicazioni per rilevare comportamenti anomali e potenziali incidenti di sicurezza. L'analisi dei log, supportata da strumenti automatici di correlazione e allarme, deve essere eseguita per identificare attività sospette. Qualsiasi evento che indichi un potenziale incidente di sicurezza deve essere gestito secondo la "PRO Procedura di gestione degli incidenti di sicurezza delle informazioni".

Uso accettabile delle informazioni e degli asset

Regole Generali di Utilizzo

Tutto il personale e le terze parti che utilizzano asset informativi di Partech devono attenersi alle regole definite nel "Codice di condotta" e nella presente politica. L'uso delle risorse aziendali è consentito esclusivamente per scopi lavorativi autorizzati.

Protezione dei Dispositivi Endpoint

Il Responsabile IT / Infrastructure & Operations deve garantire che tutti i dispositivi endpoint (es. laptop, desktop) siano protetti da minacce. Le misure di protezione devono includere:

- **Protezione da Malware**: Implementazione e manutenzione di software anti-malware, con scansioni periodiche e aggiornamenti automatici delle firme.

- **Controllo dei Dispositivi**: Applicazione di policy per la gestione sicura dei dispositivi, inclusa la protezione delle informazioni archiviate, elaborate o accessibili tramite di essi.

Installazione e Gestione del Software

L'installazione di software sui sistemi operativi è soggetta a controllo. Il Tecnico - Sistemista deve gestire l'installazione del software in modo sicuro, consentendo unicamente l'uso di applicazioni approvate e presenti in una whitelist gestita dal Responsabile IT / Infrastructure & Operations. L'installazione non autorizzata di software è severamente vietata.

Filtraggio della Navigazione Web

Per ridurre l'esposizione a contenuti dannosi, l'accesso a siti web esterni deve essere gestito tramite un sistema di filtraggio. Il Responsabile IT / Infrastructure & Operations è responsabile della configurazione e della manutenzione dei profili di filtraggio, bloccando le categorie di siti ritenute rischiose o inappropriate per l'attività lavorativa.

Utilizzo dei servizi cloud

Processo di Acquisizione e Gestione

L'adozione, l'utilizzo, la gestione e la dismissione dei servizi cloud devono seguire un processo formalizzato per garantire la conformità con i requisiti di sicurezza delle informazioni di Partech.

L' Executive - Acquisti, in collaborazione con il Responsabile IT / Infrastructure & Operations e l'Executive - Cybersecurity e Privacy, ha la responsabilità di valutare la sicurezza dei fornitori di servizi cloud prima della stipula di qualsiasi accordo. Tale valutazione deve essere condotta secondo quanto previsto nella "PRO Procedura di gestione degli acquisti e delle terze parti".

Requisiti di Sicurezza Contrattuali

Gli accordi con i fornitori di servizi cloud devono definire chiaramente le responsabilità in materia di sicurezza, i livelli di servizio (SLA) e i requisiti di protezione dei dati. L'Executive - Cybersecurity e Privacy deve assicurare che i contratti includano clausole adeguate per la gestione degli incidenti, la continuità operativa e la conformità normativa.

Configurazione e Monitoraggio

Il Responsabile IT / Infrastructure & Operations deve garantire che tutti i servizi cloud siano configurati in modo sicuro, applicando i principi di hardening e minimo privilegio. L'utilizzo dei servizi cloud deve essere monitorato per rilevare attività anomale o non conformi alle policy aziendali.

Utilizzo dei supporti di memorizzazione rimovibili

Gestione e Controllo

L'uso di supporti di memorizzazione rimovibili (es. chiavi USB, dischi esterni) deve essere limitato e controllato per prevenire la perdita di dati e l'introduzione di malware. Il Responsabile IT / Infrastructure & Operations definisce quali tipologie di supporti sono autorizzate e le condizioni per il loro utilizzo.

Protezione delle Informazioni

Le informazioni classificate come sensibili o critiche, in accordo con la "POL Politica di classificazione ed etichettatura delle informazioni", devono essere crittografate prima di essere memorizzate su supporti rimovibili. Le regole per l'applicazione della crittografia sono definite nella "PRO Procedura di crittografia e gestione delle chiavi crittografiche".

Trasporto e Smaltimento

Il personale è responsabile della protezione fisica dei supporti rimovibili durante il trasporto al di fuori delle sedi aziendali. Al termine del loro ciclo di vita, i supporti devono essere resi illeggibili o distrutti fisicamente in modo sicuro. Il Responsabile IT / Infrastructure & Operations supervisiona questo processo, che è regolamentato dalla "PRO Procedura di configurazione, gestione e smaltimento degli asset" e può avvalersi di fornitori esterni qualificati.

Scrivania e schermo puliti

Protezione di Documenti e Supporti Fisici

Tutto il personale è tenuto a garantire che le informazioni sensibili o riservate, sia in formato cartaceo che su supporti di memorizzazione, non siano lasciate incustodite sulle postazioni di lavoro. I documenti devono essere riposti in modo sicuro quando non utilizzati, specialmente al di fuori dell'orario di lavoro.

Protezione degli Schermi

Tutti i dispositivi dotati di schermo (es. computer, terminali) devono essere configurati per attivare un blocco schermo protetto da password dopo un periodo massimo di 5 minuti di inattività. Il personale ha l'obbligo di bloccare manualmente la propria sessione di lavoro ogni volta che si allontana dalla postazione, anche per brevi periodi.

Gestione delle capacità

Monitoraggio e Pianificazione

Il Responsabile IT / Infrastructure & Operations ha la responsabilità di monitorare, ottimizzare e pianificare la capacità delle risorse di elaborazione, archiviazione e rete per garantire che le prestazioni e la disponibilità dei servizi IT soddisfino i requisiti attuali e futuri dell'organizzazione. Le attività di monitoraggio devono essere continue e supportate da strumenti automatici in grado di raccogliere dati sull'utilizzo delle risorse.

Gestione degli Allarmi e Adeguamento

Devono essere configurate soglie di allarme per notificare proattivamente il Tecnico - Sistemista e il Responsabile IT / Infrastructure & Operations quando l'utilizzo delle risorse si avvicina a livelli critici. A seguito di tali allarmi, o sulla base delle analisi di trend, il Responsabile IT / Infrastructure & Operations deve avviare le azioni necessarie per l'adeguamento della capacità, che possono includere l'ottimizzazione delle configurazioni esistenti o l'acquisizione di nuove risorse. Tali modifiche devono seguire la "PRO Procedura di gestione del cambiamento".

Gestione delle vulnerabilità

Identificazione e Valutazione

L'Executive - Cybersecurity e Privacy è responsabile della definizione e dell'implementazione di un processo per la gestione delle vulnerabilità tecniche. Tale processo deve includere l'identificazione proattiva delle vulnerabilità nei sistemi informativi in uso, attraverso fonti informative affidabili, scansioni periodiche e attività di penetration testing.

Ogni vulnerabilità identificata deve essere valutata in base al rischio che rappresenta per l'organizzazione, considerando la probabilità di sfruttamento e il potenziale impatto.

Trattamento e Mitigazione

Sulla base della valutazione del rischio, l'Executive - Cybersecurity e Privacy definisce le priorità di intervento e assegna al Responsabile IT / Infrastructure & Operations la responsabilità di applicare le misure di mitigazione appropriate, come l'installazione di patch di sicurezza o la modifica delle configurazioni. Le attività di remediation devono essere tracciate e documentate. Il Tecnico - Sistemista esegue operativamente le azioni di correzione sotto la supervisione del Responsabile IT / Infrastructure & Operations.

Revisione e Reporting

L'Executive - Cybersecurity e Privacy deve rivedere periodicamente lo stato di esposizione alle vulnerabilità e l'efficacia del processo di gestione, riportando i risultati alla CEO / Direzione Generale secondo quanto previsto dalla "PRO Procedura di gestione dei rischi".

Archiviazione e Aggiornamenti

Questo documento è gestito all'interno del sistema di gestione documentale aziendale. Viene sottoposto a revisione con cadenza almeno annuale, o a seguito di cambiamenti significativi nel contesto organizzativo, tecnologico o normativo, per garantirne la continua adeguatezza. Ogni aggiornamento è approvato dalla funzione competente.

Documenti di Riferimento

- Codice di condotta
- MOD Registro dei trattamenti del titolare
- POL Politica di conservazione e cancellazione delle informazioni
- POL Politica di classificazione ed etichettatura delle informazioni
- PRO Procedura di gestione e controllo degli accessi logici
- PRO Procedura di crittografia e gestione delle chiavi crittografiche
- PRO Procedura di continuità operativa e di ripristino di emergenza
- PRO Procedura di gestione delle risorse umane
- PRO Procedura di gestione degli incidenti di sicurezza delle informazioni
- PRO Procedura di gestione degli acquisti e delle terze parti
- PRO Procedura di configurazione, gestione e smaltimento degli asset
- PRO Procedura di gestione del cambiamento

- PRO Procedura di gestione dei rischi