Partech

Limitato

POL Politica dei ruoli e delle responsabilità in materia di sicurezza delle informazioni

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 definire, assegnare e comunicare in modo chiaro e univoco i ruoli, le responsabilità e le autorità in materia di sicurezza delle informazioni all'interno dell'organizzazione, affinché tutti gli aspetti di sicurezza delle informazioni siano gestiti, supervisionati e mantenuti in conformità con i requisiti della normativa applicabile.

Indice

Campo di applicazione

La presente politica definisce e assegna i ruoli e le responsabilità per la gestione della sicurezza delle informazioni all'interno di Partech. Si applica a tutto il personale, ai collaboratori esterni e a tutti i processi e sistemi che gestiscono informazioni aziendali, in conformità con il Sistema di Gestione Integrato (SGI).

Riferimenti normativi

- ISO/IEC 27001:2022
- Regolamento (UE) 2016/679 (GDPR)

Termini e definizioni

- **Asset informativo**: Qualsiasi informazione o risorsa correlata all'informazione che ha valore per un'organizzazione.
- **Disponibilità**: La proprietà di essere accessibile e utilizzabile su richiesta di un'entità autorizzata.
- **Integrità**: La proprietà di salvaguardare l'accuratezza e la completezza degli asset.
- **Riservatezza**: La proprietà per la quale le informazioni non sono rese disponibili o divulgate a individui, entità o processi non autorizzati.

Ruoli e responsabilità

- **CEO / Direzione Generale**: Approva le policy di sicurezza, definisce ruoli e responsabilità, assicura le risorse per la gestione del rischio, agisce come promotore dei piani di continuità operativa e di risposta agli incidenti, e verifica periodicamente gli indicatori di prestazione (KPI) di sicurezza e conformità.
- **Direzione**: Richiede a tutto il personale di applicare la sicurezza delle informazioni in conformità con le politiche e le procedure stabilite.
- **Executive (Acquisti)**: Verifica che i fornitori rispettino le politiche di sicurezza delle informazioni, include clausole di protezione dei dati e sicurezza nei contratti e identifica i rischi associati ai fornitori.
- **Executive (Amministrazione & Finanza)**: Garantisce che i dati contabili, fiscali e bancari siano trattati secondo criteri di riservatezza e integrità e implementa controlli interni per prevenire frodi e accessi non autorizzati.
- **Executive (Clienti Enterprise)**: Applica i controlli ISO/IEC 27001 nei processi di supporto, collabora con il team per audit e analisi dei rischi, e forma il proprio team sulle policy di sicurezza e protezione dei dati.
- **Executive (Cybersecurity e Privacy)**: Sviluppa la strategia di sicurezza, gestisce il rischio informatico, coordina la risposta agli incidenti e la formazione, e garantisce la conformità normativa (ISO 27001, GDPR, NIS2), fungendo da punto di contatto con le autorità.
- **Executive (Ricerca e Sviluppo)**: Integra i requisiti di sicurezza fin dalla fase di progettazione di nuovi prodotti e servizi ("security by design") in collaborazione con i

team IT e di compliance.

- **Executive (Risorse umane)**: Garantisce che i dipendenti ricevano un'adeguata formazione sulla sicurezza, protegge i dati sensibili dei dipendenti e promuove la cultura della sicurezza per sensibilizzare sui rischi informatici.
- **Personale delle Aree Amministrazione & Finanza, Acquisti, Risorse Umane, Commerciale**: Gestisce le informazioni della propria area di competenza in modo sicuro e riservato, applicando le direttive e le procedure operative pertinenti.
- **Responsabile Commerciale**: Assicura la protezione dei dati dei clienti, garantendo che siano trattati in modo sicuro e conforme alle normative, identifica i rischi per la sicurezza nelle trattative commerciali e nei contratti e garantisce la conformità del proprio team alle policy di sicurezza.
- **Responsabile Forense e Cybersecurity**: Collabora all'implementazione e sorveglia processi, politiche e controlli per proteggere la riservatezza, l'integrità e la disponibilità dei dati, identificando minacce e vulnerabilità e definendo misure di mitigazione.
- **Responsabile IT / Infrastructure & Operations**: Implementa e gestisce i controlli tecnici di sicurezza, inclusi hardening, patching, gestione delle identità, backup e ripristino, segmentazione della rete, logging e capacity planning.
- **Responsabile Privacy & GDPR**: Coordina le attività per la conformità al GDPR, gestisce i registri dei trattamenti, le valutazioni d'impatto (DPIA), le violazioni dei dati (data breach), la formazione e gli audit, fungendo da punto di contatto per gli interessati e le autorità di controllo.
- **Responsabile di Area - DBA - Supporto e Progetti - Consulenza e Servizi**: Gestisce i rischi operativi legati alla sicurezza delle informazioni, assicurando che le policy di sicurezza siano integrate nei processi quotidiani e collaborando per implementare le misure di protezione dei dati.
- **RLS (Rappresentante dei Lavoratori per la Sicurezza)**: Promuove la consapevolezza tra i lavoratori sui comportamenti sicuri nella gestione delle informazioni e raccoglie segnalazioni relative a pratiche rischiose.
- **RSGI (Responsabile Sistema di Gestione Integrato)**: Governa il Sistema di Gestione Integrato (es. ISO 9001, ISO/IEC 27001), coordina gli audit interni ed esterni, monitora gli indicatori di performance e gestisce i piani di miglioramento.
- **RSPP (Responsabile del Servizio di Prevenzione e Protezione)**: Collabora alla valutazione dei rischi fisici e ambientali per le aree che ospitano infrastrutture IT critiche e alla definizione dei piani di emergenza che impattano sulla disponibilità dei sistemi.
- **Tecnico - Sistemista**: Assicura la sicurezza e la protezione dei dati aziendali e dei clienti durante la gestione e manutenzione delle infrastrutture IT, implementando le procedure tecniche per prevenire l'esposizione a rischi.
- **Tutto il Personale**: Applica le politiche di sicurezza nelle attività quotidiane, protegge gli asset informativi e segnala tempestivamente qualsiasi incidente, anomalia o debolezza di sicurezza osservata.

Definizione dei ruoli e delle responsabilità

Principi Generali di Responsabilità

Partech definisce e assegna i ruoli e le responsabilità in materia di sicurezza delle informazioni per garantire la protezione degli asset informativi e la conformità con la "POL Politica di sicurezza delle informazioni".

- **Responsabilità della Direzione**: La Direzione, a tutti i livelli gerarchici, dovrà richiedere a tutto il personale di applicare la sicurezza delle informazioni in conformità con le politiche e le procedure stabilite dall'organizzazione.
- **Responsabilità Individuale**: Tutto il personale e i collaboratori esterni sono tenuti a comprendere e ad adempiere alle proprie responsabilità in materia di sicurezza delle informazioni, come definite nella presente politica e nel "Codice di condotta". La mancata osservanza di tali doveri può comportare azioni disciplinari.

Direzione Generale (Top Management)

- **CEO / Direzione Generale**:
  - Dovrà approvare la "POL Politica di sicurezza delle informazioni" e le politiche tematiche che ne derivano.
  - Dovrà assicurare che i ruoli, le responsabilità e le autorità in materia di sicurezza delle informazioni siano definiti, comunicati e integrati nella struttura organizzativa, come formalizzato nel "MOD Mansionario".
  - Dovrà garantire la disponibilità delle risorse necessarie per l'implementazione, il mantenimento e il miglioramento continuo del Sistema di Gestione Integrato (SGI)
  - Dovrà agire come promotore (sponsor) dei piani strategici di sicurezza, inclusi quelli definiti nella "PRO Procedura di continuità operativa e di ripristino di emergenza" e nella "PRO Procedura di gestione degli incidenti di sicurezza delle informazioni".
  - Dovrà verificare periodicamente gli indicatori di prestazione (KPI) relativi alla sicurezza e alla conformità, come definito nella "PRO Procedura delle misurazioni e del monitoraggio".

Ruoli di Gestione del Sistema (Compliance e Governance)

- **RSGI (Responsabile Sistema di Gestione Integrato)**:
  - Dovrà governare il Sistema di Gestione Integrato, assicurando la conformità agli standard di riferimento, ISO 27001 e ISO 9001.
  - Dovrà coordinare gli audit interni ed esterni, come descritto nella "PRO Gestione audit interni", e gestire le non conformità e le azioni correttive.
  - Dovrà supervisionare la gestione controllata della documentazione di sistema, in accordo con la "PRO Procedura di gestione delle informazioni documentate".
- **Executive (Cybersecurity e Privacy)**:
  - Dovrà sviluppare e proporre per approvazione le strategie e le politiche per proteggere le infrastrutture, i dati e gli applicativi aziendali.
  - Dovrà coordinare il processo di valutazione e trattamento del rischio informatico, come stabilito nella "PRO Valutazione rischi per la sicurezza delle informazioni".

- Dovrà coordinare la risposta agli incidenti di sicurezza, attivando e gestendo il processo descritto nella "PRO Procedura di gestione degli incidenti di sicurezza delle informazioni".
- Dovrà promuovere la cultura della sicurezza attraverso programmi di formazione e sensibilizzazione per tutto il personale.
- Dovrà garantire l'aderenza dell'organizzazione alle normative applicabili (es. GDPR, NIS2) e agli standard come ISO/IEC 27001.
- Dovrà fungere da punto di contatto con le autorità competenti in materia di cybersecurity e privacy, in collaborazione con il "Responsabile Privacy & GDPR".

- **Responsabile Privacy & GDPR**:
  - Dovrà coordinare le attività per assicurare la conformità al GDPR e alle altre normative sulla protezione dei dati personali.
  - Dovrà collaborare all'identificazione dei rischi relativi al trattamento dei dati personali e proporre misure di mitigazione.
  - Dovrà coordinare le azioni in caso di violazione dei dati personali (data breach), assicurando la notifica alle autorità e agli interessati, ove necessario.
  - Dovrà supervisionare la gestione delle richieste degli interessati e assistere nella conduzione delle Valutazioni d’Impatto sulla Protezione dei Dati (DPIA).

Ruoli Manageriali e di Area (Management & Executive)

- **Responsabile di Area - DBA - Supporto e Progetti - Consulenza e Servizi**:
  - Dovrà assicurare che le politiche di sicurezza delle informazioni siano integrate nei processi operativi quotidiani delle rispettive aree di competenza.
  - Dovrà collaborare all'identificazione e alla mitigazione dei rischi operativi legati alla sicurezza delle informazioni.
  - Dovrà collaborare con il Responsabile IT / Infrastructure & Operations e l' "Executive (Cybersecurity e Privacy) per implementare le misure di protezione dei dati.
- **Responsabile Commerciale**:
  - Dovrà garantire la protezione delle informazioni dei clienti e dei dati commerciali sensibili, assicurando che siano trattati in conformità alle normative e alle politiche aziendali.
  - Dovrà identificare i rischi per la sicurezza delle informazioni nelle trattative commerciali e nei contratti, includendo clausole adeguate in collaborazione con l'area Acquisti e Cybersecurity.
  - Dovrà garantire che il personale dell'area commerciale sia formato e rispetti le politiche di sicurezza, segnalando ogni anomalia secondo la "PRO Procedura di gestione dei rilievi ed eventi".
- **Executive (Amministrazione & Finanza)**:
  - Dovrà garantire che i dati contabili, fiscali e bancari siano trattati secondo i principi di riservatezza e integrità, come definito nella "POL Politica di classificazione ed

etichettatura delle informazioni".

- Dovrà implementare e supervisionare controlli interni per prevenire frodi e accessi non autorizzati ai sistemi finanziari.

- **Executive (Risorse umane)**:
  - Dovrà assicurare che le responsabilità di sicurezza delle informazioni siano incluse nelle descrizioni dei ruoli e comunicate durante il processo di assunzione, come da "PRO Procedura di gestione delle risorse umane".
  - Dovrà garantire la protezione dei dati personali dei dipendenti e promuovere la formazione continua sulla sicurezza, in linea con la "POL Politica delle risorse umane sulla sicurezza delle informazioni".
- **Executive (Acquisti)**:
  - Dovrà verificare che i fornitori rispettino le politiche di sicurezza di Partech, come definito nella "POL Politica di gestione delle terze parti".
  - Dovrà includere clausole contrattuali relative alla sicurezza delle informazioni e alla protezione dei dati negli accordi con le terze parti, secondo la "PRO Procedura di gestione degli acquisti e delle terze parti".
- **Responsabile IT / Infrastructure & Operations**:
  - Dovrà implementare e gestire i controlli tecnici di sicurezza, inclusi hardening dei sistemi, gestione delle patch, segmentazione delle reti, backup e ripristino, in accordo con la "POL Politica di sicurezza operativa".
  - Dovrà gestire il ciclo di vita degli accessi logici secondo la "PRO Procedura di gestione e controllo degli accessi logici".
  - Dovrà garantire la corretta configurazione e manutenzione dell'infrastruttura di rete, come descritto nella "PRO Procedura di gestione della sicurezza della rete".
- **Executive (Clienti Enterprise)**:
  - Dovrà assicurare l'applicazione dei controlli di sicurezza ISO/IEC 27001 nei processi di supporto e progettazione per i clienti Enterprise.
  - Dovrà formare e sensibilizzare il proprio team sulle policy di sicurezza e sulle buone pratiche per la protezione dei dati dei clienti.
- **Executive (Ricerca e Sviluppo)**:
  - Dovrà integrare i requisiti di sicurezza fin dalla fase di progettazione di nuovi prodotti e servizi ("security by design"), in linea con la "PRO Procedura di sviluppo sicuro" e la "PRO Gestione progettazione".
- **Responsabile Forense e Cybersecurity**:
  - Dovrà sorvegliare l'adesione a standard e best practice nelle attività di informatica forense e nei servizi di cybersecurity erogati ai clienti.
  - Dovrà collaborare all'implementazione e alla sorveglianza dei controlli per proteggere la riservatezza, l'integrità e la disponibilità dei dati gestiti.

Ruoli Operativi e Personale (Staff Layer)

- **Tutto il Personale**:
  - Dovrà applicare le politiche di sicurezza delle informazioni nelle proprie attività quotidiane.
  - Dovrà proteggere gli asset informativi aziendali e dei clienti da accessi, modifiche o divulgazioni non autorizzate.
  - Dovrà segnalare tempestivamente qualsiasi incidente, anomalia o debolezza di sicurezza osservata al proprio responsabile e secondo la "PRO Procedura di gestione degli incidenti di sicurezza delle informazioni".
  - Dovrà utilizzare le risorse informatiche in modo appropriato e sicuro, rispettando il "Codice di condotta" e le procedure operative.
- **Tecnico - Sistemista**:
  - Dovrà assicurare la sicurezza e la protezione dei dati aziendali e dei clienti durante le attività di gestione e manutenzione delle infrastrutture IT.
  - Dovrà implementare le politiche e le procedure tecniche per prevenire l'esposizione delle informazioni a rischi.
- **Personale delle Aree Amministrazione & Finanza, Acquisti, Risorse Umane, Commerciale**:
  - Dovrà gestire le informazioni trattate nella propria area di competenza in modo sicuro e riservato, applicando le direttive della "POL Politica di classificazione ed etichettatura delle informazioni" e le procedure operative pertinenti.

Ruoli di Supporto alla Sicurezza

- **RSPP (Responsabile del Servizio di Prevenzione e Protezione)**:
  - Dovrà collaborare alla valutazione dei rischi fisici e ambientali per le aree che ospitano infrastrutture IT critiche (es. sale CED), come previsto dalla "PRO Procedura di sicurezza fisica e ambientale".
  - Dovrà collaborare alla definizione dei piani di emergenza che impattano sulla disponibilità dei sistemi informativi, in coerenza con la "PRO Gestione emergenze".
- **RLS (Rappresentante dei Lavoratori per la Sicurezza)**:
  - Dovrà promuovere la consapevolezza tra i lavoratori sui temi della sicurezza, inclusi i comportamenti sicuri nella gestione delle informazioni.
  - Dovrà raccogliere e comunicare ai referenti competenti eventuali segnalazioni relative a pratiche rischiose per la sicurezza delle informazioni.

Archiviazione e aggiornamenti

La presente politica è archiviata nel sistema di gestione documentale aziendale. Viene riesaminata con cadenza almeno annuale e aggiornata ogni qualvolta si verifichino cambiamenti organizzativi, tecnologici o normativi rilevanti, sotto la supervisione dell'Executive (Cybersecurity e Privacy) e con l'approvazione della Direzione Generale.

Documenti di riferimento

- Codice di condotta
- MOD Mansionario
- POL Politica di classificazione ed etichettatura delle informazioni
- POL Politica di gestione delle terze parti
- POL Politica di sicurezza delle informazioni
- POL Politica di sicurezza operativa
- POL Politica delle risorse umane sulla sicurezza delle informazioni
- PRO Gestione audit interni
- PRO Gestione emergenze
- PRO Gestione progettazione
- PRO Procedura di continuità operativa e di ripristino di emergenza
- PRO Procedura di gestione degli acquisti e delle terze parti
- PRO Procedura di gestione degli incidenti di sicurezza delle informazioni
- PRO Procedura di gestione dei rilievi ed eventi
- PRO Procedura di gestione della sicurezza della rete
- PRO Procedura di gestione delle informazioni documentate
- PRO Procedura di gestione delle risorse umane
- PRO Procedura di gestione e controllo degli accessi logici
- PRO Procedura di sicurezza fisica e ambientale
- PRO Procedura di sviluppo sicuro
- PRO Procedura delle misurazioni e del monitoraggio
- PRO Valutazione rischi per la sicurezza delle informazioni